

ОНЛАЙН-КРЕДИТ ФИРИБГАРЛИГИНИНГ КРИМИНАЛИСТИК ХАРАКТЕРИСТИКАСИ: ЎҒИРЛАНГАН ШАХСИЙ МАЪЛУМОТЛАР АСОСИДА КРЕДИТ РАСМИЙЛАШТИРИШ

Мўминов Азамат Солижонович

*Наманган вилояти Ички Ишлар Бошқармаси Ахборот-технологиялари
соҳасидаги жиноятларга қарши курашиш бошқармаси етакчи мутахассиси,
подполковник*

Аннотация: Мақолада онлайн-кредит фирибгарлигининг криминалистик жиҳатлари чуқур таҳлил этилган. 2024 йилда Ўзбекистон Республикасида 463 та ҳолат қайд этилган бўлиб, жабрланувчиларга 15 миллиард сўмдан ортиқ зарар етказилган. Тадқиқот доирасида жиноятчиларнинг асосий схемалари (телефон қўнғироғи, паспорт маълумотларини ўғирлаш, биометрик тизимларни айланиб ўтиш) системалаштирилган. Муаллиф *deepfake* технологияси, эски фотосуратлар ва сунъий интеллект воситалари орқали юз таниш тизимларини алдаш усулларини таҳлил этган. Мақолада жавобгарликни тақсимлаш масаласи кўриб чиқилган: жиноятчи, жабрланувчи ва банк ўртасидаги ҳуқуқий муносабатлар. Сингапур, Буюк Британия ва Европа Иттифоқи тажрибасига асосланиб, банкларнинг молиявий жавобгарлиги тизими таҳлил қилинган. Тадқиқот натижалари сифатида амалда қўллаш мумкин бўлган чоралар таклиф этилган: видео-идентификация, кўп босқичли скрининг, *liveness detection* тизимини такомиллаштириш, жавобгарликни тақсимлаш механизми ва жабрланувчиларни ҳимоя қилиш қонунчилигини такомиллаштириш. Тавсиялар банк тизими, ҳуқуқни муҳофаза қилувчи органлар ва қонун ижодчилари учун мўлжалланган.

Калит сўзлар: онлайн-кредит фирибгарлиги, *deepfake*, биометрик аутентификация, шахсий маълумотлар, банкларнинг жавобгарлиги, *liveness detection*, киберҳавфсизлик, жабрланувчиларни ҳимоя қилиш.

CRIMINOLOGICAL CHARACTERISTICS OF ONLINE CREDIT FRAUD: CREDIT REGISTRATION BASED ON STOLEN PERSONAL DATA

Abstract: This article provides an in-depth analysis of the criminological aspects of online credit fraud. In 2024, 463 cases were recorded in the Republic of Uzbekistan, causing damage exceeding 15 billion soums. The study systematizes the main schemes used by criminals, including phone scams, passport data theft, and biometric system bypass. The author analyzes methods used to deceive facial recognition systems through deepfake technology, old photographs, and artificial intelligence tools. The article examines the issue of liability distribution among criminals, victims, and banks. Based on the experience of Singapore, the United Kingdom, and the European Union, the system of banks' financial liability is examined. The research results propose practical measures, including video identification, multi-stage screening, improved liveness detection systems,

liability distribution mechanisms, and enhanced victim protection legislation. The recommendations are intended for the banking system, law enforcement agencies, and lawmakers.

Keywords: *online credit fraud, deepfake, biometric authentication, personal data, bank liability, liveness detection, cybersecurity, victim protection.*

КИРИШ

Замонавий молиявий тизимнинг рақамлаштириш жараёни фуқароларга қулайлик яратган бўлса-да, бир вақтнинг ўзида кибержиноятчилик учун янги имкониятлар ҳам яратди. Онлайн-кредит хизматлари сўнгги йилларда Ўзбекистон Республикасида кенг тарқалди: фуқаролар банкларга бормаи, фақат мобил илова орқали бир неча дақиқа ичида кредит олиш имконига эга бўлдилар. Бироқ, ушбу қулай тизим жиноятчилар томонидан суистеъмол қилиш учун мақсадга айланди.

Марказий Банкнинг маълумотларига кўра, 2024 йилда 463 та онлайн-кредит фирибгарлиги ҳолати қайд этилган бўлиб, жабрланувчиларга 15 миллиард сўмдан ортиқ зарар етказилган [1]. Омбудсман маълумотларига кўра, 2024 йилда бундай жиноятлар сони 2023 йилга нисбатан 42 фоизга ошган [2]. Бу ҳолат муаммонинг жиддийлигини ва чуқур таҳлилни талаб қилишини кўрсатади.

Омбудсман аппаратида 2024 йилда 156 та мурожаат тушган бўлиб, уларнинг 60 фоизида фирибгарлар ўзларини Марказий Банк ёки Click хизмати ходимлари сифатида танитиб, фуқаролардан шахсий маълумотларни олишган [3]. Энг оғир ҳолат шундаки, терговчилар томонидан банкка қарз фоизларини тўхтатиш бўйича кўрсатмалар берилганига қарамай, кўп банклар бу талабларни эътиборсиз қолдирган ва жабрланувчилардан қарзни талаб қилишда давом этган [2].

Мазкур тадқиқотнинг мақсади онлайн-кредит фирибгарлигининг криминалистик хусусиятларини аниқлаш, жавобгарлик масаласини таҳлил қилиш ва амалий чоралар ишлаб чиқиш ҳисобланади.

АДАБИЁТЛАР ТАҲЛИЛИ

Онлайн-кредит фирибгарлиги муаммоси жаҳон миқёсида тадқиқ этилмоқда. Сингапурда Пул-кредит ваколати (MAS) ва Ахборот-коммуникация ривожлантириш ваколати (IMDA) томонидан 2024 йил 16 декабрда “Умумий жавобгарлик доираси” жорий этилди [4]. Ушбу доирада молиявий муассасалар ва телекоммуникация операторлари phishing фирибгарликларидан зарар кўрган фуқароларга компенсация тўлаш мажбурияти белгиланган.

Буюк Британияда 2024 йилдан бошлаб банклар фирибгарлик қурбонларига зарарни тўлаш мажбурияти жорий этилди [5]. Янги қоидалар банк тизимига масъулиятни оширишга орқали жиноятларни аниқлаш ва олдини олиш чораларини кучайтириш мақсадида қабул қилинган. Зарарни тўлаш харажатлари пул юборувчи ва қабул қилувчи банк ўртасида 50:50 нисбатида тақсимланади.

Deepfake технологияси ва биометрик тизимларни алдаш усуллари бўйича кенг тадқиқотлар олиб борилган. Россия олимлари томонидан юз таниш тизимларини алдашнинг турли усуллари ўрганилган: махсус кўзойнак, инфрақизил диёдлар, сунъий интеллект орқали яратилган ниқоблар [6]. Сингапур тажрибасида Liveness Detection технологияси қўлланилмоқда, бу жонли одам ва рақамли тасвир ўртасидаги фарқни аниқлайди [7].

Ўзбекистон Республикасида ушбу муаммо бўйича тадқиқотлар бошланғич босқичда. Марказий Банк 2024 йил 1-ноябрдан 1-апрелгача муддатли вақтинчалик тартиб жорий этди, бу тартиб банкларга онлайн-кредит бериш жараёнида қўшимча текширувлар ўтказишни талаб қилади [8]. Бироқ, жавобгарлик масаласи ва жабрланувчиларни ҳимоя қилиш механизмлари ҳали тўлиқ ишлаб чиқилмаган.

ОНЛАЙН-КРЕДИТ ФИРИБГАРЛИГИНИНГ КРИМИНАЛИСТИК ХУСУСИЯТЛАРИ

Киберхавфсизлик маркази маълумотларига кўра, Ўзбекистонда содир этиладиган кибержиноятларнинг 4 фоизи онлайн-кредит фирибгарлигидир [9]. Ушбу жиноятларнинг асосий хусусияти шундаки, жабрланувчи кредиторга айланади ва жиноятчи топилмагунча қарзни тўлаш мажбуриятини олади.

Жиноят содир этишнинг босқичлари

1-босқич: Жабрланувчини танлаш ва бошланғич алоқа. Жиноятчилар тасодифий телефон рақамларига кўнғироқ қилишади. Улар ўзларини банк, давлат органи, ёки Click/Раume каби тўлов тизимлари ходимлари сифатида танитадилар. Одатда “ҳисобингиз блокланди”, “шубҳали операция аниқланди”, “хавфсизлик кўчирмас тизими янгиланиши керак” каби баҳоналар билан мулоқот бошланади.

2-босқич: Паспорт ва шахсий маълумотларни олиш. Жабрланувчини ишонтиргандан сўнг, жиноятчилар “текшириш учун” паспорт фотосуратини, ЖШШИРни ва бошқа шахсий маълумотларни сўрайдилар. Айрим ҳолларда фирибгарлар зарарли ҳаволаларни юборишади, жабрланувчи ҳаволани босганида, мобил қурилмасига троян дастури ўрнатилади ва бу дастур автоматик равишда паспорт фотосуратини, SMS-кодларни ва банк иловаларидан маълумотларни ўғирлайди.

3-босқич: Банк иловасида рўйхатдан ўтиш. Жиноятчилар жабрланувчининг маълумотлари ёрдамида кредит берувчи ташкилотнинг мобил иловасида янги аккаунт яратишади. Улар паспорт маълумотларини киритадилар ва биометрик тасдиқлаш босқичига ўтадилар.

4-босқич: Биометрик тизимни алдаш. Энг муҳим ва техник жиҳатдан мураккаб босқич. Жиноятчилар қуйидаги усуллардан фойдаланадилар:

а) Эски фотосуратлардан фойдаланиш. Айрим оддий биометрик тизимлар фақат юзнинг умумий хусусиятларини текширади, жонли одам ёки фотосурат эканлигини аниқлай олмайди. Агар банк иловасида Liveness Detection (жонликни

аниқлаш) тизими заиф ёки мавжуд бўлмаса, жинойтчи оддий паспорт фотосуратини камерага тутиб юбориши мумкин.

б) Deepfake технологияси. Илғор жинойтчилар сунъий интеллект воситаларидан фойдаланиб, жабрланувчининг юзини видео форматда қайта яратишади. Улар ижтимоий тармоқлардан ёки ўғирланган фотосуратлардан фойдаланиб, FaceSwap ёки DeepFaceLab каби дастурлар орқали жонли видео таҳлид қилишади. Ушбу видеони реал вақт режимида камерага кўрсатиб, тизимни алдашади.

в) Силикон ниқоблар ва 3D-принтерлаш. Энг мураккаб усул. Жинойтчилар жабрланувчининг юз контурига мос келувчи силикон ёки латекс ниқоб тайёрлайдилар. Бундай ниқоблар орқали мимикани ҳам таҳлид қилиш мумкин: кўз қисиш, табассум ва бошқа ҳаракатлар. 2016 йилда Шимолий Каролина университети тадқиқотчилар Facebook'дан олинган тасодифий фотосуратлар асосида 3D-муляжлар яратиб, 5 тадан 4 та юз таниш тизимини алдашлари мумкин бўлганини исботладилар [10].

5-босқич: Кредит расмийлаштириш. Биометрик тасдиқлаш муваффақиятли амалга оширилгандан сўнг, жинойтчилар кредит учун ариза тўлдирадилар. Улар одатда максимал миқдорда кредит олишга ҳаракат қилишади. Кредит тасдиқлангач, маблағ жинойтчининг картасига ўтказилади.

6-босқич: Маблағни ечиб олиш ва йўқолиш. Кредит маблағи олингандан сўнг, жинойтчилар бир неча соат ичида барча пулни нақд ҳолда ечиб олишади ёки криптовалютага айлантиришади. Улар мобил рақамни блоклайдилар ва йўқолиб кетишади. Жабрланувчи бир неча кун ёки ҳафта ўтгач, банкдан қарз тўлаш ҳақида хабар олганида, ўзининг номида кредит олинганини билиб қолади.

ЖАВОБГАРЛИК МАСАЛАСИ: КИМ АЙБДОР?

Онлайн-кредит фирибгарлигида уч томон мавжуд: жинойтчи, жабрланувчи ва банк. Ҳар бир томоннинг масъулият даражасини аниқлаш мураккаб ҳуқуқий масала ҳисобланади.

Жинойтчининг жавобгарлиги

Шубҳасиз, асосий айбдор жинойтчидир. Ўзбекистон Республикаси Жинойт кодексининг 168-моддаси фирибгарлик учун жавобгарликни белгилайди. Бироқ, амалда жинойтчини топиш ва судга тортиш мураккаб. 2024 йилда 463 та ҳолат қайд этилган бўлса-да, фош этилиш даражаси жуда паст. Жинойтчилар кўпинча чет элда, махсус дастурий таъминотдан фойдаланиб, VPN орқали фаолият юритадилар.

Жабрланувчининг “айбдорлиги”?

Баъзи банклар ва ҳуқуқшунослар жабрланувчини "эҳтиётсиз бўлганлиги" учун айблайдилар: Нега паспорт фотосуратини юбордингиз?, Нега ҳаволани босдингиз?, Нега номаълум одамга ишондингиз?. Бироқ, бу ёндашув бир қатор сабабларга кўра нотўғри:

Биринчидан, фирибгарлар психологик манипуляция усулларини профессионал даражада қўллайдилар. Улар шошилиш вазият яратиб, одамни

хаяжонли ҳолатида қолдирадилар. “Ҳисобингиз 10 дақиқадан кейин блокланади”, “Кимгадир сизнинг картангиздан 5 миллион сўм ўтказилмоқда” каби иборалар орқали жабрланувчи мантиқий фикрлаш имконини йўқотади.

Иккинчидан, кўпчилик фуқаролар технология соҳасида чуқур билимга эга эмас. Қишлоқ жойларида яшовчи, кекса ёшдаги ёки кам таълимли фуқаролар учун “зарарли ҳавола”, “deepfake”, “биометрик аутентификация” тушунчалари номаълум. Уларни бундай фирибгарликка қарши ҳимоясиз қолдириш адолатсизликдир.

Учинчидан, жабрланувчи ҳеч қачон кредит олишни истамаганини, шартномани имзоламаганини ва маблағни олмаганини қонун асосида исботлаши мумкин. Агар жиноят содир этилган бўлса, жабрланувчи қарз тўлаш мажбуриятига эга бўлмаслиги керак.

Банкнинг жавобгарлиги

Банкларнинг жавобгарлиги энг мунозарали масала ҳисобланади. Банклар ўз ҳимоя қиладиган нуқтаи назарларини қуйидагича асослайдилар: “Биз барча техник талабларга риоя қилдик”, “Биометрик тизим муваффақиятли тасдиқланди”, “Жабрланувчи ўзи маълумотларини берди”. Бироқ, қуйидаги фактлар банкларнинг масъулиятини кўрсатади:

а) Заиф биометрик тизим. Агар банк иловасида Liveness Detection тизими мавжуд бўлмаса ёки у заиф бўлса, банк ўз мажбуриятини бажармаган ҳисобланади. Замонавий технологиялар жонли одам ва фотосурат ўртасидаги фарқни аниқлаш имконини беради. Агар банк бу тизимни жорий этмаган бўлса, у фойда олиш учун хавфсизликни қурбон қилган.

б) Тезкор кредит бериш жараёни. Кўпгина банклар рақобатда устунлик қилиш учун “5 дақиқада кредит” каби хизматларни реклама қиладилар. Бироқ, ушбу тезлик хавфсизликни камайтиради. Агар кредит бир неча дақиқада тасдиқланса, бу қўшимча текширувлар ўтказилмаганлигини англатади.

в) Шубҳали ҳолатларни эътиборсиз қолдириш. Агар кредит учун ариза янги яратилган аккаунтдан, янги қурилмадан, ғайритабиий вақтда (масалан, тунда соат 3:00 да) келиб тушса ва максимал миқдорда кредит сўралса – бу аниқ шубҳали ҳолат. Автоматик скрининг тизими бундай ҳолатларни аниқлаши ва қўшимча текшириш ўтказиши керак эди.

г) Терговчиларнинг кўрсатмаларини бажармаслик. Омбудсман маълумотларига кўра, кўп ҳолларда терговчилар банкка жабрланувчидан фоизларни ундирмаслик тўғрисида ёзма кўрсатма берганига қарамай, банклар бу талабни бажаришмаган [2]. Бу Жиноят-процессуал кодексининг 36-моддасини бузишдир ва банк томонидан қонунга нисбатан масъулиятсизликни кўрсатади.

БАНКЛАРНИНГ ЖАВОБГАРЛИГИ: ХАЛҚАРО ТАЖРИБА

Сингапур модели: “Умумий жавобгарлик доираси”

Сингапур 2024 йил 16-декабрда “Shared Responsibility Framework” (Умумий жавобгарлик доираси)ни жорий этди [4]. Бу тизим бўйича молиявий муассасалар

ва телекоммуникация операторлари phishing фирибгарликларидан зарар кўрган фуқароларга компенсация тўлаш мажбуриятини олдилар.

"Каскад" (waterfall) ёндашуви: Компенсация мажбурияти қуйидаги тартибда аниқланади:

1. Агар банк ўз мажбуриятларини бажармаган бўлса (масалан, Liveness Detection тизимини жорий этмаган, шубҳали операцияларни блокламаган), у тўлиқ зарарни тўлайди.

2. Агар банк барча мажбуриятларини бажарган бўлса, лекин телекоммуникация оператори фирибгар SMS-ларни блокламаган бўлса, оператор тўлиқ зарарни тўлайди.

3. Фақат банк ва оператор ўз мажбуриятларини тўлиқ бажарган ҳолда, агар жабрланувчи ўзи эҳтиётсизлик кўрсатган бўлса (масалан, ихтиёрий равишда паролни берган), у ўзи зарарни кўради. Бироқ, бундай ҳолларда ҳам жабрланувчи суд орқали даъво қилиш ҳуқуқига эга.

Сингапур тажрибасида диққатга сазовор жиҳати шундаки, компенсация миқдори учун лимит йўқ. Агар банк ёки оператор ўз мажбуриятини бажармаган бўлса, у қанча катта зарар бўлмасин, тўлиқ тўлаши шарт [11].

Буюк Британия модели

Буюк Британияда 2024 йилдан бошлаб тўлов тизимлари регулятори томонидан янги қоидалар жорий этилди [5]. Бу қоидалар бўйича банклар авторизация қилинган тўлов фирибгарликлари (APP scams) қурбонларига зарарни тўлаш мажбуриятини олдилар. Зарар харажатлари пул юборувчи ва қабул қилувчи банк ўртасида 50:50 нисбатида тақсимланади.

Бу ёндашув банкларни ҳимоя тизимларини яхшилашга рағбатлантиради. Агар банк фирибгарликни аниқлашда муваффақиятсиз бўлса, у зарарнинг ярмини тўлайди. Шу сабабли банклар сунъий интеллект асосида шубҳали операцияларни аниқлаш тизимларини фаол ривожлантиришмоқда.

Европа Иттифоқи

Европа Иттифоқида PSD2 (Payment Services Directive 2) директиви бўйича, агар истеъмолчи ҳисобга кириш маълумотларини тўғри ҳимоя қилмаган бўлса, унинг жавобгарлиги 50 Еврога чекланган [12]. Бошқа ҳолларда банк тўлиқ зарарни тўлайди. Бу ёндашув истеъмолчиларни ҳимоя қилишга қаратилган, чунки 50 Евро – бу кўпчилик кишилар учун минимал миқдор ва бу уларни банкротликка олиб келмайди.

ОНЛАЙН-КРЕДИТ ФИРИБГАРЛИГИНИ ОЛДИНИ ОЛИШ ЧОРАЛАРИ

Халқаро тажрибани таҳлил қилиш ва Ўзбекистон шароитини ҳисобга олган ҳолда, қуйидаги амалий чоралар таклиф этилади. Ҳар бир таклиф танқидий таҳлилдан ўтказилган ва фақат реал амалга ошириш мумкин бўлган чоралар киритилган.

1-чора: Биометрик тасдиқлашда видео-идентификация

Муаммо: Фотосурат асосидаги биометрик тизим осон алданади. Оддий Liveness Detection ҳам deepfake технологияси орқали айланиб ўтилиши мумкин.

Таклиф: Муайян миқдордан юқори кредитлар учун (масалан, 10 миллион сўмдан ортиқ) видео-идентификация мажбурий қилинсин. Бу шунчаки жонли видео эмас, балки банк операторлари билан реал вақт режимида суҳбат бўлиши керак.

Механизм:

– Ариза берувчи илова орқали кредит сўрайди.

– Тизим автоматик равишда видео-қўнғироқ вақтини белгилайди (масалан, 30 дақиқадан кейин).

– Банк оператори видео орқали ариза берувчининг паспорти билан юзини солиштиради, бир неча савол беради: "Кредит учун нима мақсадда фойдаланмоқчисиз?", "Сизнинг иш жойингиз қаерда?".

– Оператор шубҳали белгиларни аниқласа (масалан, одам жуда асабий, саволга жавоб бера олмайди, ниқоб кийган), аризани рад этади.

Танқидий баҳолаш: Бу таклиф реал ва арзон. Видео-қўнғироқ технологияси аллақачон мавжуд (Zoom, Skype каби). Банкларда call-марказ ходимлари бор. Қўшимча харажат минимал – фақат операторларни махсус тренинг ўтказиш керак. Салбий томони: кредит олиш жараёни бир неча соатга чўзилади, бу баъзи мижозларни безовта қилиши мумкин. Бироқ, хавфсизлик қулайликдан муҳимроқ.

2-чора: Liveness Detection тизимини такомиллаштириш

Муаммо: Оддий Liveness Detection тизими фақат "юз ҳаракат қиляптими" деб текширади. Бу етарли эмас.

Таклиф: Марказий Банк томонидан барча банкларга минимал Liveness Detection талаблари белгилансин:

– Кўз қисишни аниқлаш (voluntary eye blink) – бу ҳаракат deepfake орқали қийинроқ таҳлид қилинади.

– Бошни ҳаракатлантиришни текшириш – чапга, ўнга, юқорига, пастга.

– Тасодифий рақамларни овозли айтишни сўраш – бу овоз ва юз тасдиқловчи қўшади.

– Инфрақизил сенсор (IR sensor) ёрдамида экран ёруғлигини аниқлаш – агар камера олдида бошқа экран бўлса (масалан, deepfake видео қўйилган телефон), IR сенсор бунини аниқлайди.

Танқидий баҳолаш: Ушбу технологиялар мавжуд ва кўплаб хорижий компаниялар томонидан ишлаб чиқилган. Бироқ, муаммо: бу технологиялар қиммат ва импорт қилиниши керак. Ўзбекистонда локал ишлаб чиқариш йўқ. Оптимал ечим: Марказий Банк хорижий компаниялар билан шартнома тузиб, барча банкларга бир хил тизимни тақдим этиши. Харажат банклардан йиғилса, ҳар бир банк учун арзонроқ бўлади.

3-чора: Кўп босқичли скрининг тизими

Муаммо: Бир босқичли автоматик тасдиқлаш тизими шубҳали ҳолатларни аниқлай олмайди.

Таклиф: Кредит бериш жараёнини уч босқичга ажратиш:

1-босқич: Автоматик скрининг. Тизим қуйидаги шубҳали белгиларни текширади:

- Янги яратилган аккаунт (1 соатдан кам вақт олдин рўйхатдан ўтган)
- Янги қурилмадан кириш
- Ғайритабиий вақт (соат 23:00 дан 06:00 гача)
- Максимал миқдорда кредит сўраш
- Сўнгги 7 кун ичида бир хил шахсга бир неча кредит аризаси

Агар шу белгилардан 2 таси ёки кўпроғи аниқланса → 2-босқичга ўтказиш.

2-босқич: 24 соатлик кечиктириш. Шубҳали ҳолатда ариза дарҳол тасдиқланмайди. Тизим 24 соатлик кутиш вақтини жорий этади. Бу вақт ичида жабрланувчи агар фирибгарлик қурбони бўлган бўлса, ўзига келиши ва банкка мурожаат қилиши мумкин. Шу билан бирга, тизим қўшимча текшириш ўтказиши: Кредит реестри орқали шахснинг аввалги кредит тарихини текшириш, телефон рақами орқали шахснинг ҳақиқий эканлигини тасдиқлаш.

3-босқич: Оператор билан суҳбат. Агар 24 соатдан кейин ҳам шубҳалар бартараф этилмаса, банк оператори ариза берувчи билан боғланади ва бир неча савол беради. Агар жавоблар мантиқсиз ёки шубҳали бўлса, ариза рад этилади.

Танқидий баҳолаш: Бу таклиф тўлиқ реал. Автоматик скрининг оддий дастурий таъминот орқали амалга оширилади. 24 соатлик кечиктириш ҳеч қандай қўшимча харажат талаб қилмайди. Оператор билан суҳбат – бу аллақачон мавжуд call-марказ хизмати. Салбий томони: ҳақиқий мижозлар учун кредит олиш жараёни секинлашади. Бироқ, Марказий Банк маълумотларига кўра, 1-ноябрдан 20-январгача "совутиш даври" жорий этилгандан кейин 285 миллиард сўмлик фирибгарлик олдини олинди [3]. Бу таклиф самарадорлигини исботлайди.

4-чора: Жавобгарликни тақсимлаш механизми

Муаммо: Ҳозирда қонунчиликда аниқ жавобгарлик механизми йўқ. Банк ва жабрланувчи ўртасида низо юзага келганда, суд жараёни узоқ давом этади.

Таклиф: Сингапур модели асосида "Каскад жавобгарлик" тизимини жорий этиш. Марказий Банк ва Адлия вазирлиги биргаликда қуйидаги тартибни белгилаши мумкин:

а) Банкнинг текшириш мажбуриятлари:

- Liveness Detection тизимини жорий этиш
- Автоматик скрининг тизими (янги аккаунт, янги қурилма, максимал кредит)
- 10 миллион сўмдан ортиқ кредитлар учун қўшимча тасдиқлаш

б) Жавобгарлик тартиби:

1. Агар банк юқоридаги мажбуриятлардан бирортасини бажармаган бўлса → банк тўлиқ зарарни тўлайди.

2. Агар банк барча мажбуриятларини бажарган бўлса, лекин жабрланувчи ўзи ихтиёрий равишда маълумот берган бўлса (масалан, SMS-кодни айтган,

паролни берган) → банк 50% компенсация тўлайди, жабрланувчи 50% ўзи кўради.

3. Агар жабрланувчи ҳеч қандай ҳаракат қилмаган (масалан, мобил қурилмасига троян дастури ўрнатилган ва автоматик маълумотлар ўғирланган) → банк тўлиқ зарарни тўлайди.

Танқидий баҳолаш: Бу таклиф қонунчилик ўзгаришини талаб қилади. Марказий Банк ва Адлия вазирлиги биргаликда махсус қонун лойиҳасини ишлаб чиқиши керак. Реал эмасми? Йўқ, тўлиқ реал. Сингапурда бу тизим 2024 йил 16-декабрда жорий этилди. Буюк Британияда 2024 йилдан бошлаб ишляпти. Ўзбекистонда ҳам амалга ошириш мумкин. Муаммо: банклар қаршилиқ кўрсатиши мумкин, чунки бу уларга қўшимча харажат. Лекин бу харажат уларни ҳимоя тизимларини яхшилашга мажбур қилади, натижада умумий жиноятлар камаяди.

5-чора: Жабрланувчиларни ҳимоя қилиш қонунчилигини такомиллаштириш

Муаммо: Омбудсман маълумотларига кўра, терговчилар банкка жабрланувчидан фоизларни ундирмаслик тўғрисида кўрсатма берганига қарамай, банклар бу талабни бажаришмаган [2].

Таклиф: Жиноят-процессуал кодексига қўшимча киритиш: Агар терговчи жабрланувчини “фуқаролик даъвогар” деб тан олган бўлса, банк автоматик равишда кредит бўйича барча операцияларни (фоизлар, жарима, асосий қарз) тўхтатиши шарт. Ушбу талабни бажармаслик учун банк ёки масъул ходимга жиноий жавобгарлик (Жиноят кодексининг

314-моддаси – суд ёки терговнинг қонуний талабларини бажармаслик).

Танқидий баҳолаш: Бу таклиф жуда осон амалга оширилади. Фақат қонунчиликка бир модда қўшиш керак. Ҳеч қандай қўшимча харажат йўқ. Салбий томони йўқ. Самарадорлиги юқори: агар банк жиноий жавобгарликдан қўрқса, следчининг кўрсатмасига дарҳол бўйсунди.

ХУЛОСА

Онлайн-кредит фирибгарлиги замонавий молиявий тизимнинг жиддий муаммоси ҳисобланади. 2024 йилда Ўзбекистон Республикасида 463 та ҳолат қайд этилган бўлиб, жабрланувчиларга 15 миллиард сўмдан ортиқ зарар етказилган. Муаммонинг ўсиш суръати (2023 йилга нисбатан 42%) тизимли ечим зарурлигини кўрсатади.

Тадқиқот натижасида қуйидаги асосий хулосаларга келинди:

Биринчидан, жиноятчилар илғор технологиялардан (deepfake, троян дастурлари, психологик манипуляция) фойдаланиб, мураккаб схемалар асосида ҳаракат қилмоқдалар. Оддий фотосурат асосидаги биометрик тизимлар бу таҳдидларга қарши самарасиз.

Иккинчидан, жавобгарлик масаласи ҳуқуқий жиҳатдан аниқ белгиланмаган. Ҳозирги ҳолатда жабрланувчи кредитор сифатида қолади ва жиноятчи топилмагунча қарзни тўлаш мажбуриятини олади. Бу адолатсиз ва ижтимоий жиҳатдан хавфли вазият яратади.

Учинчидан, халқаро тажриба (Сингапур, Буюк Британия, Европа Иттифоқи) самарали ечимлар мавжудлигини кўрсатади. “Умумий жавобгарлик доираси” тизими банкларни ҳимоя чораларини такомиллаштиришга мажбур қилади ва фуқароларни ҳимоя қилади.

Тўртинчидан, таклиф этилган чоралар техник жиҳатдан амалга ошириш мумкин ва молиявий жиҳатдан арзон: видео-идентификация, Liveness Detection тизимини такомиллаштириш, кўп босқичли скрининг, жавобгарликни тақсимлаш механизми ва қонунчиликни такомиллаштириш.

Бешинчидан, Марказий Банкнинг “совутиш даври” тажрибаси (1-ноябрдан 20-январгача 285 миллиард сўмлик фирибгарлик олдини олинди [3]) оддий чораларнинг ҳам юқори самарадорлигини исботлайди.

Тадқиқот натижалари шуни кўрсатадики, муаммонинг ечими битта томонга масъулият юклашда эмас, балки барча томонлар ўртасида мувозанатли жавобгарлик тизимини яратишда. Жиноятчи жиноий жавобгар бўлиши керак, банк техник ҳимоя чораларини таъминлаши ва ўз мажбуриятини бажармаслик ҳолатида молиявий жавобгар бўлиши шарт, жабрланувчи эса фақат ўзи ихтиёрий равишда маълумот берган ҳолларда қисман жавобгар бўлади.

Истиқболда ушбу соҳадаги тадқиқотларни давом эттириш, технологик ечимларни янада такомиллаштириш ва қонунчилик базасини мукамаллаштириш зарур. Марказий Банк, Ички ишлар вазирлиги, Адлия вазирлиги ва тижорат банклари ўртасида самарали ҳамкорлик тизимини яратиш орқали онлайн-кредит фирибгарлигини минимал даражага тушириши мумкин.

Фойдаланилган адабиётлар рўйхати:

1. Ombudsman.uz. 2024 йилда кредит расмийлаштиришга оид фирибгарлик ҳолатлари 42 фоизга ошган [Электрон ресурс]. – 2025. – URL: <https://ombudsman.uz/ru/news/2024/01/27/2024-yilda-kredit-rasmiylashtirishga-oid-firibgarlik-holatlari-42-foizga-oshgan-ombudsman> (мурожаат қилинган сана: 07.02.2026).

2. Ombudsman.uz. Омбудсман аппарати маълумотлари [Электрон ресурс]. – 2025. – URL: <https://ombudsman.uz> (мурожаат қилинган сана: 07.02.2026).

3. Spot.uz. Банклар жабрланувчилардан онлайн-кредит бўйича қарзларни ундиришмайди [Электрон ресурс]. – 2025. – URL: <https://www.spot.uz/ru/2026/01/21/credit-fraud/> (мурожаат қилинган сана: 07.02.2026).

4. Monetary Authority of Singapore. MAS and IMDA Set Out Duties and Liability of Financial Institutions and Telcos in Mitigating Digital Scams [Electronic resource]. – 2024. – URL: <https://www.mas.gov.sg> (мурожаат қилинган сана: 07.02.2026).

5. BioCatch. Singapore Proposes Shared Fraud Loss Responsibility [Electronic resource]. – 2024. – URL: <https://www.biocatch.com/blog/mas-shared-responsibility-fraud-losses> (мурожаат қилинган сана: 07.02.2026).

6. BigDataSchool.ru. Полный Deep Fake: как обмануть систему биометрии на базе Big Data и Machine Learning [Электрон ресурс]. – 2020. – URL: <https://bigdataschool.ru/blog/biometrics-hacks-use-cases.html> (мурожаат қилинган сана: 07.02.2026).
7. NtechLab. Распознавание лиц для банков [Электрон ресурс]. – 2023. – URL: <https://ntechlab.ru/solution/finance/> (мурожаат қилинган сана: 07.02.2026).
8. Ўзбекистон Республикаси Марказий Банки. Вақтинчалик тартиб онлайн-кредитлашда фирибгарликларни олдини олиш тўғрисида [Электрон ресурс]. – 2024. – URL: <https://cбу.uz> (мурожаат қилинган сана: 07.02.2026).
9. Gazeta.uz. Киберқиноятлар кундан-кунга кўпайиб, унинг турлари 18 тадан 62 тага чиқди [Электрон ресурс]. – 2025. – URL: <https://www.gazeta.uz/ru/2025/11/06/cybersecurity/> (мурожаат қилинган сана: 07.02.2026).
10. FutureCrew.ru. Распознавание лиц: как обманывают биометрические системы [Электрон ресурс]. – URL: <https://futurecrew.ru/blog/raspoznavanie-lic-kak-obmanuvayut-biometricheskie-sistemy> (мурожаат қилинган сана: 07.02.2026).
11. AO Shearman. Combatting payment account fraud: Singapore's Shared Responsibility Framework [Electronic resource]. – 2025. – URL: <https://www.aoshearman.com/en/insights/ao-shearman-on-fintech-and-digital-assets/combating-payment-account-fraud-singapores-shared-responsibility-framework> (мурожаат қилинган сана: 07.02.2026).
12. The Singapore Law Gazette. Fraudulent Transactions in an Online World [Electronic resource]. – 2021. – URL: <https://lawgazette.com.sg/feature/fraudulent-transactions-in-an-online-world/> (мурожаат қилинган сана: 07.02.2026).