DOI: https://doi.org/10.37547/supsci-ojss-05-03-32 Pages: 241-247

Oriental Journal of Social Sciences

ORIENTAL JOURNAL OF SOCIAL SCIENCES

journal homepage:
https://www.supportscience.uz/index.php/ojss

CERTAIN ASPECTS OF CYBERCRIMES COMMITTED BY BANK EMPLOYEES AND IT SPECIALISTS

Sherzod Qosimov
applicant, lieutenant colonel
Research Institute of Criminology of the Republic of Uzbekistan
Tashkent, Uzbekistan

ABOUT ARTICLE

Key words: information technology, bank employees, IT specialists, internet, cyberattack, mobile applications, cybercrime, internet fraud, internet theft, criminal code.

Received: 22.03.25
Accepted: 24.03.25
Published: 26.03.25

Abstract: The article discusses crimes committed through internet networks, foreign experiences in preventing cybercrimes perpetrated by bank employees and IT specialists, current issues in the qualification of crimes committed via internet networks in our country, as well as proposals for improving and utilizing a unified legislative practice in this field in the future and supplementing criminal legislation.

КИБЕРЖИНОЯТЛАРНИ БАНК ХОДИМЛАРИ ВА IT МУТАХАСИСЛАРИ ТОМОНИДАН СОДИР ЭТИЛИШИНИ АЙРИМ ЖИХАТЛАРИ

Шерзод Қосимов
мустақил изланувчи, подполковник
Ўзбекистон Республикаси Криминология тадқиқот институти
Тошкент, Ўзбекистон

МАҚОЛА ҲАҚИДА

Калит сўзлар: ахборот технологиялар, банк ходимлари, IT мутахасислари интернет, киберҳужум, мобиль иловалар, кибержиноятчилик, интернет фирибгарлик, интернет ўғрилик, жиноят кодекси.

Аннотация: Мақолада интернет тармоқлари орқали содир этилаётган жиноятлар, кибержиноятларни банк ходимлари ва IT мутахасислари томонидан содир этилишини олдини олиш юзасидан чет эл тажрибалари, ҳозирги кунда мамлакатимизда интернет тармоқлари орқали содир этилаётган жиноятларни квалификациясида юзага келаётган муоммолар, келгусида ушбу сохада такомиллаштириб ягона қонунчилик амалиётидан фойдаланиш ва жиноят қонунчилигини тўлдириш юзасидан таклифлар ҳақида сўз юритилган.

НЕКОТОРЫЕ АСПЕКТЫ СОВЕРШЕНИЯ КИБЕРПРЕСТУПЛЕНИЙ СОТРУДНИКАМИ БАНКОВ И IT-СПЕЦИАЛИСТАМИ

Шерзод Қосимов
соискатель, подполковник
Исследовательский институт криминологии Республики Узбекистан
Ташкент, Узбекистан

О СТАТЬЕ

Ключевые слова: информационные технологии, сотрудники банка, IT-специалисты, интернет, кибератака, мобильные приложения, киберпреступность, интернет-мошенничество, интернет-воровство, уголовный кодекс.

Аннотация: В статье рассматриваются преступления, совершаемые через интернет-сети, зарубежный опыт предотвращения киберпреступлений, совершаемых сотрудниками банков и IT-специалистами, проблемы, возникающие в настоящее время в нашей стране при квалификации преступлений, совершаемых через интернет-сети, а также предложения по совершенствованию в будущем единой правоприменительной практики в этой сфере и дополнению уголовного законодательства.

Сўнги йилларда ахборот-коммуникация технологиялари ҳаётимизга жадал суръатлар билан кириб келмоқда. Ривожланиш шу даражада шиддатли авж олмоқдаки бундан бир неча йиллар аввал бирон-бир зарурий маҳсулотни уйдан чиқмасдан интернет тармоқлари орқали харид қилиш имконияти вужудга келишини тасаввур қилиш ҳам қийин эди. Бугунги кунга келиб мамлакатимизда “рақамли иқтисодиёт”ни ривожлантириш ва телекоммуникация соҳаси тараққиётига алоҳида эътибор қаратилиб аҳолини сифатли телекоммуникация ва интернет хизматлари билан таъминлаш орқали нафақат махсулотлар, балки хизматларни ҳам ахборот-коммуникация технологиялари орқали сотиш ва харид қилиш имконияти пайдо бўлмоқда. Ўзбекистон Республикасида замонавий ахборот-коммуникация технологияларини жамиятнинг барча сохаларига жорий этиш ҳамда улардан фойдаланиш фуқароларнинг ахборотга ортиб бораётган талаб-эхтиёжларини янада тўлароқ қондириш, жахон ахборот жамиятига кириш, ҳамда жахон ахборот ресурсларидан фойдаланишни кенгайтириш учун қулай шарт-шароитлар яратилмоқда.

Ўзбекистон Республикаси Президентининг қатор фармон ва қарорлари, Вазирлар Махкамасининг бир қатор қарорлари, хусусан, Ўзбекистон Республикаси Президентининг “2022-2026-йилларга мўлжалланган Янги Ўзбекистоннинг тараққиёт стратегияси тўғрисида”ги фармонида ҳам ахборот-коммуникация технологияларини янада ривожлантиришга алоҳида эътибор қаратилган.

Булардан ташқари мамлакатимизда соғлом интернет-муҳитига эга ахборотлашган жамиятни ривожлантириш, миллий сайтларни кўпайтиришга алоҳида эътибор қаратилмоқда. Интернетда миллий веб-сайтларни яратишга қаратилган кўрик-танловларнинг ўтказилаётгани, веб-ихтирочиларнинг моддий ва маънавий жиҳатдан қўллаб-қувватланаётгани, соғлом ахборот муҳитини таркиб топтиришга йўналтирилган турли тадбирлар ўтказилиб шахсларни интернет ҳамлаларидан ҳимоялаш, ахборот олиш ва тарқатиш маданиятини тарғиб қилиш, тармоқ хавфсизлигини таъминлаш юзасидан бир қанча чора-тадбирлар амалга оширилмоқда.

Шунингдек, оммавий ахборот воситалари орқали мунтазам равишда интернет тармоқларидан фойдаланиш қоидалари, веб-макондаги хавф ва фирибгарликларга қарши курашиш усуллари тушунтирилмоқда.

Бироқ ушбу ўзгаришлар ҳаёт сифатини яхшилаш билан бир қаторда, жиноятчиликнинг янги шакли "Интернет тармоқлари орқали содир этилаётган жиноятлар"ни юзага келишига замин яратиб ҳаётимизга “кибержиноятчилик” тушунчасини олиб кирди.

Ўзбекистон Республикасининг “Киберхавфсизлик тўғрисида”ги қонунининг 3-моддасида кибержиноятчилик тушунчасига шундай таъриф берилган: унга кўра, кибержиноятчилик-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.

Ушбу қонун асосида Ўзбекистон Республикасида киберхавфсизлик соҳасидаги муносабатлар тартибга солиниб, кибержиноятларнинг олдини олиш, киберҳужумдан ҳимояланиш ҳамда кибержиноятчилик ва киберҳужумнинг олдини олишда халқаро ҳамкорликни йўлга қўйишда муҳим асос бўлиб хизмат қилмоқда.

Бироқ статистик маълумотларга назар ташласак мамлакатимизда 2024 йилда жами 58,8 мингта **киберхавфсизлик йўналишида жиноятлар содир этилган бўлиб ушбу турдаги жиноятларнинг** 97,7 фоизи фуқароларнинг банк пластик карталаридаги пулларни қўлга киритиш билан боғлиқдир.

Бинобарин, мамлакатимизда ҳозирги кунда банк пластик карталаридаги пулларни номаълум шахслар томонидан ғайриқонуний равишда қўлга киритишда ифодаланган интернет фирибгарлик ва интернет ўғрилик жиноятлари асосий мавзулардан бирига айланган бўлиб жамиятга жуда катта хавф келтириб чиқармоқда. Ушбу жиноятлар электрон тижорат сайтлари ва телеграм каналларида маҳсулотларни онлайн олди-сотди

муносабатлари орқали, ижтимоий тармоқларда турли хилдаги ютуқли ўйинлар, акциялар ва электрон савдоларни амалга ошириш орқали, хайрия мақсадлари ниқоби остида интернет ижтимоий тармоқ саҳифаларида очилган турли кўринишдаги сохта беъморлар учун фуқароларнинг банк пластик карталаридан ўз ҳисоб рақамларига пул ўтказиш орқали, фуқароларнинг банк пластик карта рақами реквизитлари, амал қилиш муддати ва бошқа шахсий маълумотларини яширин йўллар билан қўлга киритиш орқали содир этилмоқда.

Юқоридагилардан кўришимиз мумкинки, жабрланувчи банк пластик картаси махсус кодларини кибержиноятчига ишониб топширади кибержиноятчи эса ўз навбатида интернет тармоқларидан фойдаланган ҳолда унга ишониб топширилган код орқали жабрланувчига тегишли бўлган банк пластик картасидаги маблағларни бемалол тасарруф этиш имкониятини қўлга киритиб ўзганинг мулкига ёки мулкий ҳуқуқларига ғайриқонуний тарзда эга бўлади.

Бу борада Ички ишлар ходимлари томонидан фуқаролар ўртасида мазкур жиноятни қурбони бўлмаслик юзасидан тарғибот ташвиқот ишлари олиб борилмоқда. Бироқ жамият ривожланган сари фуқароларни банк пластик карталари орқали муомила қилишлари ортиб бормоқда. Шу сабабли мазкур турдаги жиноятларни олдини олишда тарғибот ташвиқот ишлари билан биргаликда процессинг марказлари (“HUMO” ва “UzCard”) маъсулиятини ошириб банк пластик карталарини техник химоя чораларини кучайтириш лозим деб ўйлайман.

Бундан ташқари ушбу содир этилаётган жиноятларни банк ходимлари ва IT мутахасислари томонидан содир этилиши янада ушбу жиноятни хавфлилик даражасини оширади. Чунки ушбу турдаги тоифа вакиллари ўзларининг содир этаётган жиноятларини якунлаш учун бор имкониятларини ишга солиб чуқур билим ва кўникмага эга бўладилар ҳамда ўз фаолиятларини технологик тараққиётга мослаштириб борадилар. Улар профессионал жиноятчилар сифатида ушбу турдаги жиноятлардан яшириниш технологияларини яхши эгаллаганликлари сабабли жиноятларни узоқ вақт аниқланмасдан қолишига шу билан бирга уларни янгитдан шунга ўхшаш жиноятларни содир этишда давом этишларига замин яратади. Натижада эса уларнинг фаолиятининг ягона воситаси жиноят натижасида топилган пул ресурслари бўлиб уларнинг даромадининг асосий манбаига айланади.

Шунингдек ушбу тоифадаги жиноятчилар ўзларининг махсус билимлари ва тизимга кириш имкониятларидан фойдаланиб, жиноятни (масалан, маълумот ўғирлаш, пул

ўтказиш) осон ва самарали восита сифатида кўрадилар. Мисол учун, IT мутахассиси тизимдаги заифликни топиб, ўзининг шахсий манфаатлари йўлида фойдаланиши мумкин.

Бир марта муваффақиятли жиноят содир этган IT мутахассиси ёки банк ходими бу фаолиятни одатий холга айлантириши натижасида, уларнинг қонуний иши маош эмас, балки жиноят асосий "касб"га айланади.

Натижада фуқаролар томонидан давлат олдидаги ишончсизлик кўпайиб хизматларнинг камайишига олиб келади.

Энди бевосита чет эл амалиётида IT мутахассиси ёки банк ходимлари томонидан кибер жиноятларни содир этилишини олдини олиш борасидаги чора-тадбирларни кўриб чиқамиз;

АҚШда банк ва молия тизимларида кибер жиноятларнинг олдини олиш учун SOX (Sarbanes-Oxley Act) ва PCI DSS (Payment Card Industry Data Security Standard) каби қатъий стандартлар жорий қилинган. Бу стандартлар ходимларнинг фаолиятини доимий мониторинг қилиш, маълумотларга рухсатсиз киришни чеклаш ва ички аудитни кучайтиришни талаб қилади.

Сингапурда банк секторида Behavior Analytics ва AI асосидаги тизимлар кенг қўлланилади. Бу тизимлар ходимларнинг одатий фаолият тарзини ўрганади ва шубҳали ҳаракатлар (масалан, рухсатсиз транзакция) аниқланса, дарҳол хабар беради. Натижада ички жиноятлар тез аниқланиб бартараф этилади. Бу технологиялар банк тизимининг хавфсизлигини оширади, лекин харажатнинг юқорилиги ва техник мутахассисларга эҳтиёж туғдиради.

Германияда банк ходимлари ва IT мутахассислари учун мунтазам киберхавфсизлик тренинглари ўтказилиб турилади. Масалан, BaFin (Федерал молиявий назорат органи) қоидаларига кўра, ходимлар кибер хавфлардан хабардор бўлиши ва ахлоқий нормаларга риоя қилишлари шарт. Натижада ходимларнинг жиноий ниятлари камайиб қонуний оқибатлардан хабардор бўлишади. Аммо бу жараён узоқ муддатли бўлиб доимий ресурслар талаб қилади.

Хитойда 2017 йил 1 июнда кучга кирган қонунга асосан барча молиявий муассасалар, шу жумладан банклардан маълумотлар хавфсизлигини таъминлаш, ходимларнинг фаолиятини назорат қилиш ва кибертаҳдидларга қарши чоралар кўришни тақозо қилади. Қонунга кўра банк ходимлари ва IT мутахассислари махфий маълумотларга рухсатсиз кириш ёки уларни ташқи томонларга ўтказишда қатъий жавобгарликка тортилади. Бундан ташқари Хитойда банк секторида AI ва Behavior Analytics тизимлари кенг қўлланилади. Масалан, ICBC (Industrial and Commercial Bank of

China) каби йирик банклар ходимларнинг фаолиятини реал вақтда кузатиш учун машинали ўқитиш алгоритимларидан фойдаланади. Ушбу тизимлар ходимларнинг одатий фаолият тарзини (масалан, транзакциялар вақти, маълумотларга кириш частотаси) ўрганади ва шубхали харакатлар (масалан, рухсатсиз маълумот юклаш) аниқланса, дарҳол хавфсизлик хизматларига хабар беради. Хитойда банк ходимлари ва IT мутахассислари учун доимий текширув (background checks) ўтказилади. Шунингдек уларнинг иш жойидаги фаолияти видеокамералар ва белгиланган тизим асосида ўрганилиб уларга қаътий жавобгарлик юклатилади ва уларнинг шахсий молиявий аҳволи ҳам мунтазам текширилади. Бу уларнинг жиноий фаолиятга мойиллигини камайтиради. Келгусида ходимлар томонидан содир этилиши мумкун бўлган салбий ходисаларни олдини олиш мақсадида ходимларга мунтазам равишда киберхавфсизлик бўйича тренинглар ўтказилиб жиноят натижасида етказилган қонуний оқибатлар тушунтирилади.

Юқоридагилардан келиб чиқиб ва чет эл тажрибасини Ўзбекистон Республикасига мослаштириш борасида келгусида банк ходимлари ва IT мутахассислари томонидан содир этилиши мумкун бўлган кибержиноятларни олдини олиш борасида қуйидагича таклифлар илгари сурилади;

– Ҳозирги кундаги ахборот-коммуникация технологиялари соҳаси бўйича мутахасислар тайёрлаб бераётган олий ва ўрта-махсус таълим ўқув юртлари талабалари ва уларнинг битирувчилари томонидан мазкур турдаги жиноятларни содир этилишини олдини олиш мақсадида уларни ҳуқуқий онгини шакллантириш, талабалар онгида кибержиноятлар содир этилиши қонунчилик билан тақиқланганлиги ва тегишли жавобгарликни келтириб чиқариши юзасидан илмий асосланган ягона ўқув қўлланмалари ҳамда мафкуравий йўналиш ишлаб чиқиш;

– Ўзбекистонда банк ходимлари ва IT мутахассислари учун киберхавфсизлик бўйича Ўзбекистон Банклар Ассоцияцияси ҳамда Давлат Хавфсизлик Хизмати билан ҳамкорликда модулли ўқув дастурлари ишлаб чиқилиб қисқа муддатли курслар ташкил қилинишини ва ушбу курсларда ходимлар онгида кибержиноятлар содир этилиши қонунчилик билан тақиқланганлиги ва тегишли жавобгарликни келтириб чиқариши юзасидан билимларни шакллантириш;

– Ўзбекистон Республикаси жиноят кодексининг 168-моддасининг 4-қисми “б” бандида кўрсатилган “ўта хавфли рецидивист” жумласини “ ўта хавфли рецидист ёки мазкур модданинг 3-қисми “г” бандида назарда тутилган жиноятни ахборот тизими, ахборот технологиялари юзасидан ўқувдан ўтган ҳамда масъул шахслар томонидан” жумласига алмаштириш;

– Ўзбекистон Республикаси жиноят кодексининг 168-моддасининг 5-қисмида етказилган моддий зарарнинг ўрни қопланган тақдирда озодликни чеклаш ва озодликдан маҳрум қилиш тариқасида жазо қўлланилмаслиги кўрсатилган бўлиб агарда шахс фирибгарлик жиноятини ахборот тизими, ахборот технологиялари орқали содир этган тақдирда истисно тариқасида ушбу қоида амал қилмаслиги, фақатгина етказлиган зарарнинг қопланиши жазо тайинланаётганда эътиборга олиниши, шунингдек ахборот тизимидан, шу жумладан ахборот-коммуникация технологияларидан фойдаланиб содир этилган жиноятларга жазо тайинлаётганда асосий жазодан ташқари қўшимча жазо сифатида муайян ҳуқуқдан маҳрум қилиш (интернет тармоқларидан фойдаланмаслик) жазо қўлланиши таклифини бераман.

Мамлакатимизда олиб борилаётган ислоҳотлар замирида халқ фаровонлиги ётар экан, халқ фаровонлигини таъминлаш, аҳолининг давлат органларига бўлган ишончини янада ошириш, олиб борилаётган ислоҳотларни янада такомиллаштириш интенет орқали содир этилаётган жиноятларга қарши курашиш бўйича ислоҳотларни янги босқичга кўтариш мақсадга мувофиқдир.

Фойдаланилган адабиётлар

1. Ўзбекистон Республикаси Конституцияси.-Тошкент “Ўзбекистон”.-2020.
2. Ўзбекистон Республикаси Жиноят кодекси https://www.lex.uz/acts/111453
3. А.У.Анорбоев. Кибержиноятчилик, унга қарши қарши курашиш муаммолари ва киберхавфсизликни таъминлаш истиқболлари; монография, тошкент 2020 й
4. Эхтиёт бўлинг, ижтимоий тармоқларда фирибгарлик\ http://www.qoshrabot.uz/o-z/node/661
5. Ш.М.Мирзиёевни ЎзЛДПнинг X қурултойида сўзлаган нутқи. https://uznews.uz/posts/2030-iilgaca-savkat-mirziyoev
6. Ш.М.Мирзиёевни Олий Мажлисга Мурожаатномаси. https://uza. Uz,30.12.2020
7. https://daryo.uz/k/2025/02/26/zoravonlikda-odam-savdosiga ozbekistonda-2024-yilda-sodir-etilganjinoyatlar-statistikasi-ochiqlandi
8. https://www.pcisecuritystandards.org/document_library
9. https://www.bafin.de/SharedDocs/Downloads/EN/Aufsicht/dl_bait_en.pdf
10. www.chinalawtranslate.com/en/cybersecurity-law-of-the-peoples-republic-of-china
11. https://www.icbc-ltd.com/en/investor/annual_reports/