ЎЗБЕКИСТОН РЕСПУБЛИКАСИ ЭЛЕКТРОН ТЎЛОВ ТИЗИМЛАРИДАГИ ҲУҚУҚБУЗАРЛИКЛАРГА ҚАРШИ КУРАШ ЖАРАЁНЛАРИДА ҚЎЛЛАШ УЧУН ХОРИЖИЙ ДАВЛАТЛАР ТАЖРИБАСИ ТАҲЛИЛИ

Ўрмонов Рустамжон Таввакалжон ўғли
Ахборот хавфсизлиги йўналиши бўйича мустақил тадқиқотчи,
электрон почта манзили: urmonovrustamjon84@gmail.com

Аннотация: Ушбу мақолада электрон тўлов тизимларидаги ҳуқуқбузарликларга қарши кураш бўйича халқаро тажриба ва хорижий давлатлар тажрибаси таҳлил қилинди. Шунингдек, Россия Федерацияси тажрибасининг элементлари батафсил ёритилди ҳамда Ўзбекистон шароитида қўллаш имкониятлари асосланди.

Калит сўзлар: тўлов тизимлари, кибержиноятчилик, киберфирибгарлар, Будапешт Конвенцияси, онлайн фирибгарлик, ижтимоий муҳандислик.

АНАЛИЗ ОПЫТА ЗАРУБЕЖНЫХ СТРАН ДЛЯ ИСПОЛЬЗОВАНИЯ В ПРОЦЕССЕ БОРЬБЫ С НАРУШЕНИЯМИ В ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СИСТЕМАХ РЕСПУБЛИКИ УЗБЕКИСТАН

Аннотация: В данной статье проанализирован международный опыт и опыт зарубежных стран по борьбе с нарушениями в электронных платежных системах. Также подробно освещены элементы опыта РФ и обоснованы возможности применения в условиях Узбекистана.

Ключевые слова: платежные системы, киберпреступность, кибермошенники, Будапештская конвенция, онлайн-мошенничество, социальная инженерия.

ANALYSIS OF THE EXPERIENCE OF FOREIGN COUNTRIES FOR USE IN THE PROCESS OF COMBATING VIOLATIONS IN ELECTRONIC PAYMENT SYSTEMS OF REPUBLIC OF UZBEKISTAN

Abstract: This article analyzed the international experience and the experience of foreign countries in combating violations in electronic payment systems. Also, the elements of the experience of the Russian Federation were covered in detail and the possibilities of application in the conditions of Uzbekistan were justified.

Keywords: payment systems, cybercrime, cyber fraudsters, Budapest Convention, online fraud, social engineering.

Барча соҳаларда бўлганлиги каби электрон тўлов тизимларидаги жиноятларга қарши кураш механизмини такомиллаштиришда ҳам ушбу

йўналишда муаммоларни самарали ҳал қилган ёки таҳдидлар табиати бўйича Ўзбекистон Республикасидаги муаммоларга яқин бўлган хорижий давлатлар тажрибасини ўрганиш тадқиқот натижаларининг мустаҳкамланишига хизмат қилади.

Ахборот-коммуникация технологиялари соҳасида содир этилаётган жиноятлар трансчегаравий табиатга эга эканлигини инобатга олиб, уларнинг олдини олиш учун норматив-ҳуқуқий йўналишдаги халқаро ҳамкорликнинг йўлга қўйилиши ҳам муҳим аҳамиятга эга. Хусусан, миллий қонунчиликни унификация қилиш, кибержиноятчиликка қарши кураш методлари ва халқаро ҳамкорликни ривожлантириш мақсадида 2001 йилнинг 23 ноябрида “Кибержиноят тўғрисида”ги Конвенция[1] (Будапешт Конвенцияси) қабул қилинган. Ушбу Конвенция дастлаб минтақавий аҳамиятга эга бўлган. Бугунги кунга келиб, у халқаро аҳамиятдаги ҳужжат сифатида эътироф этилади ҳамда 68 та давлат ушбу ҳужжатни ратификация қилган. Марказий Осиё давлатларидан Қозоғистон Республикаси мазкур Конвенцияга қўшилиш учун таклиф қилинган. Ушбу ҳужжатнинг кейинчалик алоҳида соҳаларни тартибга солиш бўйича ривожланиб борганлигини кузатиш мумкин. Хусусан, 2003 йилнинг 28 январида “Компьютер тизимларидан фойдаланган ҳолда ирқчилик ва ксенофобик характердаги ҳаракатларни жиноий жавобгарликка тортиш тўғрисида”ги конвенцияга қўшимча протокол[2] ва 2022 йилнинг 5 декабрида “Кибержиноят тўғрисидаги конвенцияга ҳамкорликни кенгайтириш ва электрон далилларни ошкор қилиш” бўйича иккинчи қўшимча протокол[3] имзоланган.

Мазкур Конвенциянинг 13-моддасида барча аъзо давлатлар миллий қонунчиликларида кибержиноятларни олдини олиш учун кибермаконда жисмоний шахслар томонидан содир қилинган ҳуқуқбузарликлар учун озодликдан махрум қилиш жазоси тайинлашни ва юридик шахслар учун молиявий санкциялар қўллашни жорий қилишлари шартлиги белгиланган.

Шунингдек, Конвенциянинг 14-моддасида кибермакондаги барча ҳуқуқбузарликлар жиноий жавобгарлик доирасида кўриб чиқилиши ва суд томонидан жазо тайинланиши амалиётини норматив-ҳуқуқий жиҳатдан йўлга қўйиш кўрсатилган.

Бундан ташқари, Конвенциянинг 8-моддасида компьютер технологияларидан фойдаланган ҳолда фирибгарлик қилганлик учун

[1] Конвенцию о компьютерных преступлениях. Будапешт, 23 ноября 2001 года. url: https://rm.coe.int/1680081580

[2] Дополнительный протокол к Конвенции о преступлениях в сфере компьютерной информации, об инкриминировании расистских актов и совершенного ксенофоба при помощи информационных систем (CEL №189). url: https://rm.coe.int/1680081611

[3] Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224). url: https://www.coe.int/en/web/conventions/full-list?module= treaty-detail&treatynum=224

жавобгарликни миллий қонунчиликда акс эттириш қайд қилинган.

Масалан, Россия Федерацияси мазкур Конвенцияни ратификация қилган бўлиб, Жиноят кодексининг 159[6]-моддасида ушбу жиноят учун жавобгарлик белгиланган.

Ушбу Конвенция талабларига мувофиқ, кибержиноятчиликнинг олдини олиш борасида хорижий давлатлар томонидан 3 та асосий модел ишлаб чиқилган.

Биринчи модел – давлатнинг интернет тармоғи устидан тўлиқ назоратини ўрнатишида намоён бўлади.

Хусусан, Хитой Халқ Республикасида интернет тўлиқлигича ҳукумат назоратида ҳисобланиб, ҳукумат серверлари бошқа давлатда жойлашган ижтимоий тармоқлар, веб-саҳифалардан фойдаланишга чеклов ўрнатади ҳамда давлат ҳудудида фойдаланилаётган барча провайдерлар устидан тўлиқ назоратни амалга оширади.

Ҳозирда мазкур моделнинг айрим элементларини Россия Федерацияси томонидан қўлланилишини кузатиш мумкин.

Иккинчи модел – фойдаланувчиларнинг ҳар қандай ҳаракатлари учун жавобгарликни провайдерларга юклашни назарда тутувчи кибержиноятчиликни олдини олиш усули бўлиб, бунда провайдерлар улардан фойдаланувчиларнинг ноқонуний хатти-ҳаракатларини доимий равишда ўзлари мониторинг ва таҳлил қилиб боришлари талаб қилинади.

Шунингдек, бу моделни қўллаш орқали давлат кибермаконда доимий назорат учун харажат қилмайди, аксинча провайдерларнинг мукаммал ишлашлари учун шароит яратиб, бюджетдан маълум миқдордаги маблағларни тежаши ва кибержиноятчиликни олдини олишга эришиши мумкин.

Мазкур моделнинг кенг қўлланилишини Франция тажрибасида учратиш мумкин. Ушбу амалиётга кўра провайдерларнинг доимий равишда мониторинг ва таҳлил натижасида аниқлаган маълумотларини манфаатдор учинчи шахсларга беришлари шарт.

Бундан ташқари, Францияда 1978 йилда “Информатика ва эркинликлар бўйича миллий комиссия” ташкил қилинган бўлиб, унинг вазифасида провайдерлардар ҳар қандай шахс тўғрисида маълумотларни манфаатдор учинчи шахслар томонидан амалдаги қонунчиликка мувофиқ олинаётганлигини доимий равишда мониторинг қилиши белгилаб қўйилган.

Учинчи модел – провайдерлар давлатнинг махсус органлари билан ҳамкорликда доимий равишда кибермаконда хавфсизликни таъминлаш мақсадида ўзаро ҳамкорликни амалга оширади. Яъни, интернетда ноқонуний хатти-ҳаракат ҳақида ахборот алмашинувини йўлга қўйиши орқали давлат хавфсизлигига таҳдид ҳисобланган ахборотлар интернет тармоғига

жойлаштирилган тақдирда ҳам провайдерлар жавобгарликка тортилмайди. Германия ва Япония давлатлари бугунги кунда ушбу моделдан самарали фойдаланиб келмоқда.

Юқоридагилардан ташқари "Жаҳон иқтисодиёт форуми" томонидан 2020 йилда "Хизмат кўрсатувчи провайдерлар учун кибержиноятларни олдини олиш тамойиллар"и ишлаб чиқилган. Ушбу тамойилларнинг тадқиқот предметига алоқадор бўлганларини кўриб чиқиш мумкин.

Биринчи тамойил – ҳукумат фуқароларга қарши қаратилган киберҳужумлар ҳақида огоҳлантириш, ўзларини ҳимоя қилиш учун шарт-шароит яратиш ва қўллаб-қувватлашни ўз зиммасига олади.

Иккинчи тамойил – аппарат-дастурий таъминотлар, тизим ишлаб чиқарувчилари ва сотувчилари билан яқинроқ ҳамкорликни йўлга қўйиш хавфсизликни таъминлаш даражасини оширишга имкон беради.

Бунга кўра, ҳукумат бозорга ўз маҳсулотларини олиб кираётган компанияларга қатъий равишда мукаммал аппарат-дастурий таъминотларни олиб киришини талаб қилиши лозим.

Бирлашган Араб Амирликларида киберхавфсизликни таъминлаш бўйича юқори технологияларнинг қўлланилишига қарамасдан, банк карталари билан боғлиқ фирибгарликларни содир этиш кўп учрайди. Ушбу жиноятларда ижтимоий муҳандисликнинг улуши юқори эканлигини инобатга олиб, ҳукумат томнидан ахборот компаниялари ташкил этилади. Хусусан, Абу-Даби рақамли бошқармаси ва Киберхавфсизлик кенгаши томонидан ташкил этилган ахборот компанияси доирасида "Киберхавфсизликнинг 4 та олтин қоидаси" ишлаб чиқилган ва тарғибот ишлари олиб борилган. Ушбу қоидалар қуйидагича тавсифланади:

1. Аноним абонентлар билан мулоқот қилманг.
2. Шубҳали веб-сайтларга киришдан сақланинг.
3. Битта паролни қайта ишлатманг.
4. Интернетда банк картаси ва ҳисоб рақамлари тўғрисидаги шахсий маълумотларни ҳеч қачон улашманг. Фирибгарлик ҳолатлари ҳақида 8002626 рақамига бепул мурожат қилинг[4].

Инсон омили билан боғлиқ фирибгарлик жиноятларининг олдини олишда тарғибот ишларини ташкил қилиш барча хорижий давлатлар тажрибасида устувор ҳисобланади.

Хитой Халқ Республикаси тажрибасида нисбатан жиддий чораларини кузатиш мумкин. Хусусан, ХХР Жамоат хавфсизлиги вазирлиги қошидаги фирибгарликка қарши кураш миллий Маркази томонидан мобил илова ишлаб

[4] Жителей ОАЭ научили избегать мошенников в интернете Власти ОАЭ опубликовали правила, которые помогут уберечься от кибермошенников. url: https://russianemirates.com/news/uae-news/zhiteley-oae-nauchili-izbegat-moshennikov-v-internete/

чиқилган бўлиб, ушбу илова орқали полиция чет эл молиявий сайтларидан фойдаланган абонентларни аниқлайди ва улар билан дастур орқали суҳбатлашади. Онлайн фирибгарликларнинг олдини олиш мақсадида яратилган ушбу илова ХХРда оммавий тарзда юклаб олинган ва фаол фойдаланилади[5].

Мутахассисларнинг фикрича, Россия Федерацияси тўлов тизимлари киберфирибгарларнинг имкониятларини чеклай бошлагач, ушбу уюшган жиноий гуруҳлар Марказий Осиё давлатлари, хусусан Ўзбекистон аҳолисига нисбатан ўз фаолиятини йўналтирган. Шу сабабли, ушбу йўналишда Россия Федерацияси тажрибасининг элементларидан фойдаланиш яхши самара бериши мумкин.

Бугунги кунда киберфирибгарликларга қарши кураш Россия Федерацияси учун ҳам долзарб масала бўлиб, ушбу йўналишни тартибга солиш бўйича ислоҳотлар амалга ошириб келинмоқда. Жумладан, Россия Давлат Думаси раисининг маълумот беришича, 2022 йил бошидан октябрь ойигача бўлган муддатда пластик карталар ёрдамида 72 мингдан ортиқ жиноят содир этилган. Россия Федерацияси Бош прокуратураси эса 2022 йилнинг дастлабки 11 ойида киберфирибгарликлар сони олдинги йилнинг мос даврига нисбатан 45 фоизга кўпайганини маълум қилган эди. Кейинчалик, Россия Федерацияси ИИВ пресс-маркази 2022 йилнинг сўнгида кибержиноятлар бўйича кўрсаткичлар бироз барқарорлашганлиги тўғрисида ахборот берган. Ушбу соҳадаги самарадорликнинг ошгани кузатилгани сабабли, Россия Федерациясида амалга оширилган чора-тадбирларни таҳлил қилиш ҳамда Ўзбекистон шароитида ушбу тажрибадан фойдаланиш масаласини кўриб чиқиш мумкин.

Банк карталаридаги жиноятларни олдини олиш мақсадида “Сбербанк” томонидан қуйидаги чора-тадбирларни амалга ошириш орқали ҳуқуқбузарларнинг эҳтимолий уринишларига чек қўйилган.

“Сбербанк Онлайн” тизимида доимий ва вақтинчалик мижоз паролларини киритиш учун виртуал клавиатурадан фойдаланиш тартибининг жорий қилиниши банкоматларда фирибгарлар томонидан паролни қўлга киритиш эҳтимолини кескин камайтирди.

“Сбербанк Онлайн” тизимида қўшимча тасдиқловсиз амалга оширилувчи транзакциялар миқдорига чекловлар белгилаш амалиёти жорий қилиниши орқали белгиланган миқдордан кўп бўлган ўтказмаларни тасдиқлаш учун қўшимча талаблар белгиланди (масалан: калит сўзлардан фойдаланиш).

Бундан ташқари, йирик тўловларни олувчиларни олдиндан рўйхатдан ўтказиш ва уларни ўтказишнинг қўшимча шартларини белгилаш механизмини йўлга қўйиш орқали (масалан, телефон орқали келишиш) пул ўтказмалари

[5] Китай использует приложение по борьбе с мошенничеством для отслеживания доступа к зарубежным сайтам финансовых новостей. url: https://www.ft.com/content/84b6b889-ae03-47f7-9cd0-bd604b21d5de

жараёнларига бегона шахсларнинг аралашувига чек қўйилди.

Шунингдек, ушбу йўналишдаги ҳуқубузарликларга қарши кураш бўйича қонунчилик такомиллаштирилган бўлиб, амалиётда самарасини берган. Хусусан, 2022 йил 4 октябрда Россия Федерацияси Давлат Думаси фуқароларнинг банк карталарини ўғирлашга қарши қонун лойиҳасини қабул қилди. Янги тартибнинг жорий қилиниши ўғирланган пулларни ечиб олиш учун барча ҳисоблар занжирини блоклаш жараёнларини осонлаштирди.

Янги қонунга асосан, Россия банки ва Ички ишлар вазирлиги ўртасида ўзаро ахборот ҳамкорлиги механизми яратилди. Унга кўра, Ички ишлар вазирлиги мижознинг розилигисиз пул ўтказишга уринишлар билан боғлиқ ҳаракатлар тўғрисидаги маълумотларни Марказий банкка юборади. Россия банки, ўз навбатида, маълумотлар базасидан ноқонуний операцияларни амалга оширишга уринишлар ҳақидаги маълумотларни Ички ишлар вазирлигига ўтказади. Бу тезкор-қидирув тадбирларини зудлик билан бошлаш имконини беради (амалиётда 2022 йил октябргача банклар томонидан Ички ишлар вазирлигининг ўғирлик бўйича сўровларига фақат 30 кундан кейин жавоб берилган ҳолатлар кўп бўлган). Шунингдек, ушбу қонун асосида битта жиноий иш доирасида бутун ҳисоблар занжирини блокировка қилиш имконияти яратилди. Бу жиноятчилар томонидан ўғирланган маблағларни ечиб олиш каналларини қидиришни анча мураккаблаштиради.

Бундан ташқари, қонунчиликдаги ўзгаришларга кўра, банк мижозлари фирибгарлардан ҳимояланиш учун онлайн операцияларни чеклашлари мумкин бўлди. Хусусан, улар онлайн кредитларни расмийлаштиришни таъқиқлаш ва транзакциянинг максимал миқдорини белгилаш имконига эга бўлди.

Шунингдек, янги тартиб бўйича банклар фуқароларнинг онлайн транзакцияларни амалга оширадиган барча қурилмаларини аниқлашлари, уларнинг телефон рақамлари ва электрон почта манзилларини тасдиқлашлари ҳам талаб қилинади. Хусусан, ушбу тартибга кўра, 2024 йилнинг июль ойидан бошлаб Россия Федерациясидаги банклар Россия Банки махсус базасидаги фирибгарлар ҳисоб рақамига пул ўтказмасини амалга оширган тақдирда, жабрланувчининг мурожаатидан сўнг 30 кун ичида тегишли маблағни мижозга қайтариш мажбуриятини олади. Ушбу норманинг жорий қилинишига 2023 йил давомида киберфирибгарлик жиноятларининг 50 фоизи ижтимоий муҳандислик асосида муваффақиятли амалга оширилганлиги ҳам сабаб бўлган. Амалдаги тартибга кўра, психологик босим остида кибефирибгарлик қурбони бўлган мижозларнинг маблағлари қайтарилмас эди.

Бундан ташқари, ушбу норма банкларга шубҳали ҳисоб рақамларига пул ўтказишга уринишлар кузатилганда транзакцияларни 2 суткага музлатиш ваколатини беради. Бу орқали банк томонидан шубҳали пул ўтказмаси ҳақида

огоҳлантирилган мижозда ҳаттоки фирибгарлар таъсири остида бўлса ҳам, ўйлаб кўриб, қайта қарор қабул қилишга имконият яратилади. Россия Банкининг маълумот беришича, қонун кучга киргунига қадар Россия Федерацияси Марказий банки махсус рўйхатни шакллантириш ҳамда ушбу маълумотлар билан барча банкларни таъминлаш чораларини кўради.

Юқоридагилардан ташқари, Россия Федерацияси Марказий банки томонидан банк ходимларининг кибергигиена талабларига риоя қилишларини текшириш амалиёти йўлга қўйилган ва ушбу амалиёт такомиллаштириб борилмоқда. Аввалги тартиб бўйича Россия Федерацияси Марказий банки ушбу ўқув ҳужумларини олдиндан огоҳлантирган ҳолда ўтказган бўлса, 2023 йил август ойидан буён огоҳлантиришсиз ўтказиб келмоқда. Россия банки талабига кўра, электрон тўлов ташкилотлари ахборот хавфсизлиги хизматида фаолият юритмайдиган ходимларининг электрон почталарини тақдим қилади. Марказий банк эса ушбу манзилларга зарарланган хаволаларни юборади ва жараёнга нисбатан ходимнинг муносабатини кузатади. Ушбу амалиёт орқали ходимнинг нотаниш файлни очишга уриниши баҳоланади.

Амалга оширилаётган ислоҳотларга қарамасдан Россияда ушбу йўналишдаги салбий тенденциялар кузатилмоқда. Хусусан, 2023 йилда банк ҳисоб рақамларига етказилган зарар миқдори 15,8 миллиард рублни ташкил қилган. Бу олдинги йилга нисбатан 11,5 фоизга ошган ҳисобланади. Россия банки ушбу ҳолатни телефон қўнғироқлари орқали фирибгарликларнинг мақсадли амалга оширилаётганлиги билан изоҳлаган. Яъни киберфирибгарлар банк мижозларига тегишли маълумотларни қўлга киритиш бўйича юқори самарадорликка эришмоқда. Бундан ташқари сўнгги вақтларда банк кредит карталари орқали (984800 та фирибгарлик амалиётлари аниқланган ва 7,12 миллиард рубль пул ўғирланган) пулларни ўзлаштириш, шахсий жамғармаларни ўғирлаш ҳамда фирибгарлар босими остида кредитлар расмийлаштириш каби механизмлар ҳам ривожланиб бормоқда. Мутахассислар юқоридаги салбий тенденцияларнинг ривожланиб бораётганлигини ишончли матнлар тайёрлашда ва фирибгарлар фаолиятини автоматлаштиришда сунъий интеллектдан кенг фойдаланиш, масофавий банк хизматлари мижозлари сонининг ортиб бориши ҳамда Россиядан ташқарида жойлашган қўнғироқ-марказлари (Call center) фаолиятининг такомиллашиб бориши билан изоҳламоқда.

Хулоса сифатида айтиш мумкинки, хорижий давлатлар тажрибаси элементларидан Ўзбекистон шароитига мослаштирган ҳолда фойдаланиш орқали ушбу соҳадаги қадамларни жадаллаштириш ҳамда юқорироқ даражага кўтариш мумкин. Мутахассисларнинг фикрича, Россия Федерацияси тўлов тизимлари киберфирибгарларнинг имкониятларини чеклай бошлагач, ушбу уюшган жиноий гуруҳлар Марказий Осиё давлатлари, хусусан Ўзбекистон

аҳолисига нисбатан ўз фаолиятини йўналтирган. Шу сабабли, ушбу йўналишда Россия Федерацияси тажрибасининг элементларидан фойдаланиш яхши самара бериши мумкин.

Шунингдек, мақола давомида таҳлили қилинган “Кибержиноят тўғрисида”ги Конвенция (Будапешт Конвенцияси) талабларини Ўзбекистон шароитида қўллаш ҳамда кейинчалик ушбу Конвенцияга қўшилиш масаласини кўриб чиқиш тавсия этилади.

Мақолада келтирилган таҳлил натижаларидан электрон тўлов тизимларидаги ҳуқуқбузарликларга қарши кураш механизми муаммоларига оид тадқиқот ишларида фойдаланиш мумкин.

Фойдаланилган манбалар

1. Конвенцию о компьютерных преступлениях. Будапешт, 23 ноября 2001 года. Материалы сайта www.rm.coe.

2. Дополнительный протокол к Конвенции о преступлениях в сфере компьютерной информации, об инкриминировании расистских актов и совершенного ксенофоба при помощи информационных систем (CEL №189). Материалы сайта www.rm.coe.

3. Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224). Materials of site: www.rm.coe.

4. www.russianemirates.com сайти материаллари.

5. www.ft.com сайти материаллари.