Жамият ва инновациялар –
Общество и инновации –
Society and innovations
Journal home page:
https://inscience.uz/index.php/socinov/index

The history of the emergence and development of crimes related to cyber fraud

Anvar TOSHTEMIROV[1]

Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan

ARTICLE INFO

Article history:
Received September 2022
Received in revised form
25 October 2022
Accepted 20 November 2022
Available online
25 December 2022

Keywords:
cybersecurity,
cyber fraud,
information attack,
information technology,
fraud using information technology,
electronic world,
culture of using social networks,
immunity to information security.

ABSTRACT

The article analyzes the relevance of information security today, the crime of fraud using information technology, the history of its development, and related concepts. Statistics related to fraudulent looting of property using information technology and its negative impact are also provided. The article highlights the relevance of information security today, and the tasks that need to be performed to combat the crime of fraud committed using information technology.

2181-1415/© 2022 in Science LLC.
DOI: https://doi.org/10.47689/2181-1415-vol3-iss11/S-pp95-102

Киберфирибгарлик билан боглик жиноятларнинг пайдо булиш ва ривожланиш тарихи

Калит сўзлар:
киберхавфсизлик,
киберфирибгарлик,
ахборот хуружи,
ахборот технологиялари,
ахборот технологияларидан фойдаланиб содир этилган фирибгарлик жинояти,
электрон дунё,

АННОТАЦИЯ

Мақолада ахборот хавфсизлигининг бугунги кундаги долзарблиги, ахборот технологияларидан фойдаланиб, содир этилган фирибгарлик жинояти, унинг ривожланиш тарихи ва у билан боғлиқ тушунчалар таҳлил қилинган. Шунингдек, ўзгалар мулкини ахборот технологияларидан фойдаланиб фирибгарлик йўли билан талон-торож қилиш ва унинг салбий таъсири билан боғлиқ статистик маълумотлар берилган. Ахборот хавфсизлигининг бугунги кундаги долзарблиги, ахборот технологияларидан

[1] Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan

ижтимоий тармоқдан фойдаланиш маданияти, ахборот хавфсизлиги иммунитети.

фойдаланиб содир этилган фирибгарлик жиноятига қарши курашиш бўйича амалга оширилиши лозим бўлган вазифалар ёритилган.

История возникновения и развития преступлений, связанных с кибермошенничеством

Ключевые слова: кибербезопасность, кибермошенничества, информационная атака, информационные технологии, мошенничества с использованием информационных технологий, электронный мир, культура использования социальных сетей, иммунитет к информационной безопасности.

АННОТАЦИЯ

В статье анализируется актуальность информационной безопасности на сегодняшний день, преступление мошенничества с использованием информационных технологий, история его развития и связанные с ним понятия. Также приводится статистика, связанная с мошенническим разграблением имущества с использованием информационных технологий и его негативным воздействием. Освещается актуальность информационной безопасности на сегодняшний день, задачи, которые необходимо выполнить по борьбе с преступлением мошенничества, совершенного с использованием информационных технологий.

SUMMARY

The dice of people in the social process manifest themselves in a variety of forms. Despite the fact that, on the basis of the norms of law, a respectful attitude to other people's rights and freedoms has been established that does not harm their legitimate interests, certain categories of persons, taking advantage of naivety, credulity, lack of legal knowledge of others and other similar reasons, commit crimes related to various manifestations of fraud, in particular, cyber fraud which is becoming more and more common today, unfortunately, it is noted that the number of types of crimes is growing every day.

Fraudulent looting of someone else's property using information technology is one of the most common, and currently intensively growing types of looting of someone else's property in comparison with other types.

Approaches to the concept of fraud using information technology differ in various literature, and the main approach is explained by the objective side of the crime, that is, the method of encroachment on the property. Based on this point of view, we can say that the social network, in particular the Internet system, is the main means of fraud on the way to achieving the goal.

Инсонларнинг ижтимоий жараёндаги ўзар муносабатлари турли хил кўринишларда намоён бўлади. Қонун нормалари асосида ўзгаларнинг хуқуқ ва эркинликларига нисбатан ҳурмат билан муносабатда бўлиш, қонуний манфаатларига зарар етказмаслик белиалаб қўйилишига қарамасдан, айрим тоифадаги шахслар бошқаларнинг соддалиги, ишонувчанлиги, ҳуқуқий билими етишмаслиги ва шу каби бошқа сабаблардан фойдаланиб, фирибгарликнинг

турли кўринишлари, хусусан, бугунги кунда тобора авж олиб бораётган киберфирибгарлик билан боғлиқ жиноятларни содир этаётганлиги, ачинарлиси, бундай турдаги жиноятларнинг сони кун сайин ортиб бораётгани кузатилмоқда. Хусусан, статистик маълумотлар таҳлили республика бўйича 2018 йил йилда 6483 та фирибгарлик жинояти рўйхатга олинган бўлса, 2019 йилда бу кўрсаткич 6321 тани ташкил этиб, 2,5 фоизга камайган бўлса, 2020 йилда бу рақам 10496 тани ташкил этиб, 2019 йилга нисбатан 39,8 фоизга, 2021 йилда 25270 та содир этилган бўлиб, 2020 йилга нисбатан 58,5 фоизга кўпайганлигини кўрсатмоқда. Ушбу жиноятдан 2021 йилда 25212 нафар шахслар жабрланган [1]. Фирибгарлик мулкка тажовуз қилишнинг кўринишларидан бири бўлиб, ижтимоий-хавфли харакат сифатида шароитга мослашувчанлиги, турли шаклларда намоён бўлиши, жумладан, ахборот технологияларидан фойдаланиб содир этилиши билан ҳам хавфли тусга эга ҳисобланади.

Ўзгалар мулкини ахборот технологияларидан фойдаланиб фирибгарлик йўли билан талон-торож қилиш, ўзгалар мулкини талон-торож қилишнинг бошқа турларига қараганда энг кўп тарқалган ҳамда ҳозирги кунда шиддат билан ортиб бораётган турларидан бири ҳисобланади [10].

Ахборот технологияларидан фойдаланиб содир этилган фирибгарлик тушунчасига турли адабиётларда ёндашув турлича бўлиб, асосий ёндашув жиноятнинг объектив томони, яъни мулкка тажовуз қилишнинг усули билан изоҳланган [8]. Ушбу фикрдан келиб чиқиб, айтиш мумкинки, фирибгарликнинг мақсадга эришиш йўлидаги асосий воситаси сифатида ижтимоий тармоқ, хусусан Интернет тизими асосий ўринга эга.

Жамиятда Интернет глобал тармоғининг ривожланиши, унинг барча соҳаларда кенг ўрин ва кўламга эга бўлиши, жиноят оламининг ҳам эътиборидан четда қолмади. Шу сабабли Интернет тизими ривожланиши билан бирга ундан ғайриқонуний мақсадларда фойдаланишга бўлган ҳаракат ва уринишлар ҳам доимий равишда кузатиб келинмоқда ва маълум даражада мақсадларига етишаётганини ҳам кўриш мумкин.

Интернет тармоғининг ривож топиши натижасида “Интернет хакерлиги” деган ахборот технологиялари соҳасида алоҳида тармоқ вужудга келган. Илк компьютер хакерлари 1960 йилларда Массачусетс технология институтида пайдо бўлган, дастлабки Интернет хакерлиги эса ўзларини “414 гуруҳи” (банда-414) деб номланган вояга етмаган ўспиринлар томонидан содир этилган бўлиб, улар 9 кун ичида АҚШдаги Лос-Аламос Давлат ядро қуролини ўрганиш лабораториясидаги 60 дан ортиқ шахсий компьютерларини ишдан чиқаришган. 1983 йилда эса дастлабки кибертеррористлар гуруҳи ушланган. Шу орқали 1983 йилда “Военные игры” (“WarGames”) номли дастлабки хакерлар тўғрисидаги фильм яратилган.

1983 йилда Парижда Иқтисодий ҳамкорлик ва ривожланиш ташкилотининг экспертлар гуруҳи компьютер жиноятларининг криминологик таърифини беришган ва уларнинг фикрича, компьютерлар жиноятлари автоматлаштирилган ишлов бериш ва (ёки) маълумотларни узатиш билан боғлиқ ҳар қандай ноқонуний, ахлоқий ёки рухсатсиз хатти-ҳаракатлар ҳисобланади [9].

1984 йилдан бошлаб “2600” илк хакерлар тўғрисидаги журнал мунтазам равишда чоп этила бошлаган.

1988 йили Америка компьютер ускуналари ассоциацияси 30 ноябрни “Халқаро ахборотни ҳимоя қилиш куни” деб эълон қилди. Бу кунни эълон қилишдан асосий мақсад барчага компьютер ахборотларини ҳимоя қилиш зарурлиги, шунингдек, дастурий воситалар ишлаб чиқарувчилар ва фойдаланувчилар эътиборини хавфсизлик масалаларига қаратишдан иборат эди. Таъкидлаш жоизки, бежиз ушбу кунга айнан 1988 йилда асос солинган эмас. Негаки, шу йили Моррис исмини олган “чувалчанг эпидемияси” илк бор оммавий тарзда тарқалган, яъни 1988 йилда Червь Моррис томонидан дастлабки зарарли вирус яратилган, бунинг оқибатида АҚШ ҳукумати ва университетларидаги 6000 га яқин компьютерлар ушбу зарарли вирус қурбонига айланишган. Ўша воқеадан сўнг соҳа мутахассислари ахборот хавфсизлигини таъминлаш масалаларига жиддий ёндашиш зарурлиги ҳақида ўйлай бошладилар. Ўша кундан эътиборан ҳозирга қадар компьютер ускуналари ассоциацияси ташаббуси билан бутун дунёда ахборотни муҳофаза қилишга доир турли қизиқарли тадбирлар ҳамда халқаро анжуманлар ўтказиб келинади. Шу билан бирга, тадбирларда ҳимояланмаган ускуналар келтириб чиқараётган зарарлар ҳажми ҳақида ахборот берилади.

Айнан шу воқеалардан кейин бундай зарарли фаолиятга қарши курашиш мақсадида АҚШда CERT Интернет хавфсизлигини таъминлаш маркази ташкил қилинган ва у томонидан 1988 йилда 6 та, 1989 йилда 132 та, 1990 йилда эса, 252 та киберҳодиса аниқланган [11]. 1990 йилда АҚШда “Sundevil” операцияси уюштирилиб, АҚШнинг 14 шаҳридаги хакерларга нисбатан мисли кўрилмаган ов уюштирилган. Бунинг оқибатида, 1993 йилда Лас-Вегасда хакерларнинг биринчи ҳар йили ўтказиладиган йиғилиши бўлиб ўтган [7].

Киберфирибгарлик турли замонларда турлича номлангани сабабли унинг ривожланиш тарихи ҳам жой ва маконга қисман боғлиқ бўлган, хусусан, АҚШда киберфирибгарлик ва унга қарши курашиш ўзгача ривожланган бўлса, Россия Федерациясида бошқача ривож топган. Масалани янада аниқроқ тушунтирадиган бўлсак, “Telegram”, “WhatsApp”, “Одноклассники”, “Facebook” каби ижтимоий тармоқлар аслида ўзаро мулоқот учун зарур бўлса-да, аммо уларнинг қулайлиги ва хавфсизлиги турлича бўлганлиги сабабли ҳам киберфирибгарликлар ушбу технологияларга қарши ҳужум қилишдан олдин қайси бирининг хавфсизлиги заиф эканлигини аниқлайди ва шунга қараб ўзининг кейинги ҳаракатларини олиб боради. Буни яхши англаган технология мулкдорлари эса ўзининг технологияси орқали келаётган фойдасидан қуруқ қолмаслик учун давлатдан ёрдам сўрайди, давлат ҳам ушбу технология орқали келаётган солиқ ва бошқа йиғимлардан айрилмаслик учун киберхавфсизликка оид ўз сиёсатини юритади. Мазкур киберхавфсизликка сиёсатни эса, технологиялар эмас, балки шахслар ишлаб чиққанлиги сабабли барча давлатларда киберхавфсизлик ва кибержиноятчилик ўзгача тарихга эга бўлган.

Шу ўринда Натан Ротшильднинг “ахборотга эга бўлган киши, дунёга ҳукмронлик қилади” [6], деган сўзларини эслаш орқали ушбу жараёнга бўлаётган қизиқишнинг кескин ортиб кетганлигини биргина Россия давлатидаги қуйидаги статистика тасдиқлаб турибди, яъни 1998 йилда 7 та компьютер соҳасидаги жиноятчилик рўйхатга олинган, 2020 йилда 180 153 тага, яъни 22 йил ичида 25736 баробар кўпайган.

Киберфирибгарликнинг кейинги ривожи 1999 йил январь ойида “Happy-99” номли Интернет тармоғидаги дастлабки вируснинг ихтиро қилингани бўлди. Натижада 1999 йил август ойида Хитой ва Тайвандаги компаниялар бир-бирига нисбатан ўзаро жуда кенг миқёсдаги киберҳужумлар уюштиришди. 2000 йил 1 май куни Манила шаҳрида “Мен сени севаман” номли Интернет тармоғида компьютер вируси топилди. Киберфирибгарликнинг жуда кенг ривожланиб кетишига давлатлар томонидан олиб борилган киберхавфсизликка оид сиёсат катта тўсиқ бўлган, хусусан, давлатда киберхавфсизликни таъминлаш мақсадида совуқ уруш иштирокчиси АҚШда, CERT Интернет хавфсизлигини таъминлаш маркази ташкил қилинган бўлса 1986 йилдаёқ СССР Ички ишлар вазирлиги тизимида Электрон урушларга қарши курашиш бошқармаси ташкил этилган. 1997 йилда Россия Федерацияси жиноят кодексига 28-боб компьютер маълумотлари соҳасидаги жиноятлар киритилган ва ушбу соҳадаги жиноятларга нисбатан суриштирув харакатларини олиб бориш мақсадида тезкор-қидирув бўлинмаси ташкил этилган. 1999 йилгача РФнинг 81 та таъсис тузилмаларида Ички ишлар вазирлиги, Ички ишлар бошқармаси ва Ички ишлар бўлимлари даражасига тенглаштирилган махсус таркибий тузилмалар ташкил қилинган. 2000 йилдан бошлаб, ушбу бўлимларга юридик мутахассисликдаги ходимларнинг ҳам ишга қабул қилиниши натижасида РФда мазкур соҳадаги жиноятчиликка қарши курашишнинг самарали усуллари яратилди. Шунингдек, юқоридаги бошқарма ҳам Ички ишлар вазирлиги таркибига ўтказилди [13].

Ахборот технологияларидан фойдаланиб содир этилган фирибгарликларнинг жой ва маконга, замонга ўзаро боғлиқлиги сабабли ҳам ушбу жиноятлар турли мамлакатларда турлича номланган ҳамда уларнинг таркибига турли жиноятлар киритилган. Хусусан, Японияда у икки гуруҳга ажратилган бўлиб, 1-гуруҳга компьютерларга кириш билан боғлиқ жиноятлар деб номланиб, ушбу гуруҳга компьютер фирибгарлиги, ёзувларга зарар етказиш ва бизнесга аралашиш, тўлов карталари билан боғлиқ, компьютерга рухсатсиз кириш каби жиноятлар ва 2-гуруҳга Интернет тармоғидан фойдаланиш орқали содир этиладиган жиноятлар деб номланиб, ушбу гуруҳга фирибгарлик, муаллифлик ҳуқуқининг бузилиши, ахлоқсиз характердаги одобсиз хабарлар юбориш, болалар порнографияси билан боғлиқ материалларни тарқатиш билан боғлиқ жиноятлар киритилган [12].

Францияда эса IT-технологиялари ёрдамида содир этилган, яъни маълумотларни автоматик қайта ишлаш соҳасидаги зарарли сохта банк карталари ва шахсий маълумотларни ҳимоя қилувчи паролларни клонлаш, бузиш имконини берадиган дастурий таъминот, компьютер ёки тармоклардан фойдаланиш қоидаларини бузиш, иккинчи гуруҳга эса жиноий ишларни тайёрлаш ва содир этишда рақамли технологиялардан фойдаланишга оид жиноятлар кибержиноятлар тоифасига киритилган [14].

Украинада компьютерлар, автоматлаштирилган тизимлар, компьютер тармоқлари ёки телекоммуникация тармоқларининг ишлашига ўзбошимчалик билан аралашиш, зарарли дастурий ёки аппарат воситаларини ишлатиш, тарқатиш ёки сотиш, шунингдек, маркетинг учун яратиш, рухсат берилмаган маълумотларни автоматлаштирилган тизимларда, компьютерларда, ахборот воситаларида тарқатиш ва кириш тақиқланган воситаларда сақланадиган маълумотларни тарқатиш, уларга

рухсатсиз кириш, улардан фойдаланиш, ҳимоя қилиш қоидаларини бузиш, уларнинг ишлашига тўсқинлик қилиш кибержиноятлар тоифасига киритилган [15].

Ахборот технологияларидан фойдаланиб содир этилган жиноятлар Ўзбекистон Республикаси жиноят қонунчилигида Ўзбекистон Республикасининг 2007 йил 25 декабрдаги “Ахборотлаштириш ва маълумотлар узатиш соҳасида қонунга хилоф ҳаракатлар содир этганлик учун жавобгарлик кучайтирилганлиги муносабати билан Ўзбекистон Республикасининг айрим қонун ҳужжатларига ўзгартиш ва қўшимчалар киритиш тўғрисида”ги ЎРҚ-137-сонли Қонуни билан Жиноят кодексига киритилган XX1-боб (Ахборот технологиялари соҳасидаги жиноятлар)да ўз аксини топган [4].

Шунингдек, Ўзбекистон Республикаси Президентининг 2018 йил 14 майдаги “Жиноят ва жиноят-процессуал қонунчилиги тизимини тубдан такомиллаштириш чора-тадбирлари тўғрисида”ги ПҚ–3723-сон қарори асосида, технологик тараққиёт, жумладан, кибержиноят билан боғлиқ жиноят турларининг кенгайганлиги ҳисобга олинган ҳолда ахборот технологиялари соҳасида жавобгарликни назарда тутувчи нормалар қайта кўриб чиқилди. Бунга кўра, Ўзбекистон Республикаси Жиноят кодексининг Ахборот технологиялари соҳасида содир этилган жиноятлар учун белгиланган айрим моддаларини санкция қисмига ўзгаришлар киритилган бўлса, мазкур кодекснинг “Компьютер тизимидан қонунга хилоф равишда (рухсатсиз) фойдаланиш учун махсус воситаларни ўтказиш мақсадини кўзлаб тайёрлаш ёхуд ўтказиш ва тарқатиш” деб номланган 2783-моддаси “Компьютер тизимидан, шунингдек телекоммуникация тармоқларидан қонунга хилоф равишда (рухсатсиз) фойдаланиш учун махсус воситаларни ўтказиш мақсадини кўзлаб тайёрлаш ёхуд ўтказиш ва тарқатиш” деб ўзгартирилди.

Бундан ташқари ушбу боб Ўзбекистон Республикасининг 2018 йил 22 октябрдаги “Ўзбекистон Республикасининг айрим қонун ҳужжатларига жамоат хавфсизлигини таъминлашга қаратилган ўзгартиш ва қўшимчалар киритиш тўғрисида”ги ЎРҚ–503-сон Қонунига кўра, янги 2787-модда (Телекоммуникация тармоғидан қонунга хилоф равишда (рухсатсиз) фойдаланиш) [4] билан тўлдирилди.

Шунингдек, Ўзбекистон Республикаси Президентининг 2022 йил 28 январдаги ПФ–60-сонли фармони билан тасдиқланган “Янги Ўзбекистоннинг 2022–2026 йилларга мўлжалланган Тараққиёт Стратегияси”да фуқароларнинг ахборот олиш ва тарқатиш эркинлиги борасидаги ҳуқуқларини янада мустаҳкамлаш мақсадида, кибержиноятчиликнинг олдини олиш тизимини яратиш вазифаси белгилаб берилди ва ушбу вазифани амалга оширишнинг механизмларидан бири сифатида, кибержиноятчилик учун жиноий жавобгарликни қайта кўриб чиқиш [14] лозимлиги қайд этилди. Мазкур вазифанинг ижроси юзасидан дастлабки ташланган қадамлардан бири сифатида, Ўзбекистон Республикасининг 2022 йил 19 октябрь куни қабул қилинган “Ўзбекистон Республикасининг айрим қонун ҳужжатларига ўзгартиш ва қўшимчалар киритиш тўғрисида”ги ЎРҚ–794-сон Қонунига кўра, Ўзбекистон Республикаси Жиноят Кодексининг 168-модда 2-қисм “в” банди (Компьютер техникаси воситаларидан фойдаланиб содир этилган бўлса), 168-модда 3-қисм “г” банд сифатида (Ахборот тизимидан, шу жумладан, ахборот технологияларидан фойдаланиб содир этилган бўлса) [5] ўзгартирилганлигини қайд этиш мумкин.

Ахборот технологияларидан фойдаланиб содир этилган фирибгарликнинг янги замонавий шакллари ва усулларига қарши курашиш бўйича ушбу соҳада фаолият олиб бораётган ходимлар фаолиятини самарали йўлга қўйиш муҳим аҳамиятга эга. Бу борада, ушбу соҳа вакилларининг фаолиятини ҳуқуқий жиҳатдан белгилаб берувчи қонунчилик тизимини янада такомиллаштириш, уларнинг янги инновацион технологиялардан фойдаланиш кўникмаларини доимий равишда ошириб бориш, замонавий техник таъминот бўйича кенг имкониятлар яратиш, халқаро тажрибалар алмашинувини йўлга қўйиш ва бошқа шу каби вазифалар ижросини таъминлаш муҳим аҳамият касб этади.

Ахборот технологияларидан фойдаланиб содир этилган фирибгарлик учун жавобгарликка тортилган шахсларнинг алоҳида электрон базасини ташкил этиб, жавобгарликка тортиш ва судланганлик муддати ўтмаган ушбу тоифадаги шахсларнинг маълум бир ҳуқуқларини суд томонидан чеклаш масаласини қонунчиликка киритиш зарур: жумладан, хорижга чиқишини вақтинчалик чеклаш, кредит ажратилиши билан боғлиқ масалаларни вақтинчалик чеклаш, солиқ ва бошқа мажбурий тўловларда имтиёзлар тақдим этмаслик, мулкий масалалар бўйича битимлар тузиш миқдорини чеклаш. Агар ушбу шахсларнинг белгиланган муддатларда муносиб хулқ-атворда бўлиши таъминланганда, суднинг қарорига мувофиқ ушбу ҳуқуқлари тикланиши мумкинлигига оид тартибнинг киритилиши таклиф қилинади.

Хулоса ўрнида шуни таъкидлашимиз зарурки, айнан ахборот технологияларидан фойдаланиб содир этилган фирибгарликнининг иқтисодиётга таъсири натижасида мамлакатнинг кейинги ривожига сунъий тўсиқлар юзага келади. Ушбу тўсиқларни бартараф қилмас эканмиз, юртимизда иқтисодий тангликлар кучайиб бораверади. Иқтисодий танглик эса инсонларнинг давлат органларига нисбатан ишончсизлигини ва мамлакатда турли тартибсизликлар вужудга келтириш хавфини кучайтиради.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР РЎЙХАТИ:

1. Ўзбекистон Республикаси ИИВ ҳузуридаги Тергов департаменти маълумотлари.

2. Ўзбекистон Республикаси Президентининг 2022 йил 28 январдаги “2022–2026 йилларга мўлжалланган Янги Ўзбекистоннинг Тараққиёт Стратегияси тўғрисида”ги ПФ–60-сонли фармони. https://lex.uz/docs/5841063.

3. Ўзбекистон Республикасининг 2007 йил 25 декабрдаги “Ахборотлаштириш ва маълумотлар узатиш соҳасида қонунга хилоф ҳаракатлар содир этганлик учун жавобгарлик кучайтирилганлиги муносабати билан Ўзбекистон Республикасининг айрим қонун ҳужжатларига ўзгартиш ва қўшимчалар киритиш тўғрисида”ги ЎРҚ–137-сонли Қонуни. https://lex.uz/acts/1295262?ONDATE=26.12.2007%2000#1295383 .

4. Ўзбекистон Республикасининг 2022 йил 19 октябрдаги “Ўзбекистон Республикасининг айрим қонун ҳужжатларига ўзгартиш ва қўшимчалар киритиш тўғрисида”ги ЎРҚ–794-сон Қонуни. https://lex.uz/docs/6242547.

5. https://ru.wikipedia.org/wiki/%D080.

6. А. Николаева, М. Тумбинская. Киберпреступность: история развития, проблемы практики расследования. Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ Казань, Россия. Материалы

международной конференции Sorucom 2014 // 13-17 октября 2014. https://computer-museum.ru/articles/materialy-mezhdunarodnoy-konferentsii-sorucom-2014/629/.

7. Атаманов Р.С. Основы методики расследования мошенничества в сети Интернет: Автореф. дисс... канд. юрид. наук. – Москва. 2012. – С. 28. Коломинов В.В. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа: Автореф. дисс... канд. юрид. наук. – Краснодар. 2017. – С. 25.

8. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – М.: Юрлитинформ, 2001. – 496 с.

9. Комаров А.А. Криминологические аспекты мошенничества в глобальной сети Интернет: дис. ... канд. юрид. наук / А.А. Комаров. – Пятигорск, 2011. – С. 262. Медведев С. С. Мошенничество в сфере высоких технологий: Автореф. дис. ... канд. юрид. наук. – Краснодар, 2008. – С. 21.

10. Мишина И.М. Расследование мошенничества, совершенного с использованием банковских карт: криминалистические и уголовно-процессуальные аспекты: Автореф. дис. ... канд. юрид. наук. – Москва, 2009. – С. 26.

11. Филиппов М.Н. Расследование краж и мошенничеств, совершенных с использованием банковских карт и их реквизитов: автореф. дис... канд. юрид. наук. – Москва, 2012. – С. 30.

12. Л.П.Зверянская. Исторический анализ этапов развития киберпреступности и особенности современных киберпреступлений // Научно-методический электронный журнал «Концепт». – 2016. – Т. 15. – С. 881–885. – URL: http://e-koncept.ru/2016/96090.htm.

13. Н.А. Морозов. Борьба с компьютерной преступностью в Японии // Общество и право. 2014. № 2(48). – С. 144.

14. Распоряжение Правительства Российской Федерации № 1701 -р от 22.10.99 г. «Об усилении борьбы с преступлениями в сфере высоких технологий и реализации международных договоренностей и обязательств Российской Федерации»» // СЗ РФ. – 1999. – № 44. – Ст.5335. 1https://71,xn--b1aew.xn--p1ai/Deiatelnost/Borba s kiberprestupnostiu.

15. Федоров А.В. Информационная безопасность в мировом политическом процессе: учеб, пособие. – М.: 2006. – С. 111.

16. Украина жиноят кодексининг 16-боби, 361-3631-моддаларидан. https://meget.kiev.ua/kodeks/ugolovniy- kodeks/razdel-1-16/.