Тўхтаев Сардор Султон ўғли
Жаҳон иқтисодиёти ва дипломатия университети Халқаро ҳуқуқ факультети 1-курс талабаси

РАҚАМЛИ ТЕХНОЛОГИЯЛАР СОҲАСИДАГИ ҲУҚУҚБУЗАРЛИКЛАРГА ҚАРШИ КУРАШИШ ҲАМДА АХБОРОТ ХАВФСИЗЛИГИНИ ТАЪМИНЛАШНИНГ ТАШКИЛИЙ-ҲУҚУҚИЙ ЖИҲАТЛАРИ

Тухтаев Сардор Султон угли
студент 1 курса факультета Международного права Университета мировой экономики и дипломатии,

ОРГАНИЗАЦИОННО-ПРАВОВЫЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ НАРУШЕНИЯМ В ОБЛАСТИ ЦИФРОВЫХ ТЕХНОЛОГИЙ И ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Tuxtaev Sardor
1st year course student International Law faculty, University of World Economy and Diplomacy

ORGANIZATIONAL AND LEGAL ASPECTS OF COMBATING VIOLATIONS IN THE FIELD OF DIGITAL TECHNOLOGIES AND ENSURING INFORMATION SECURITY

Аннотация. *Мақолада рақамли технологиялар, кибермакон, кибержиноят тушунчалари, унинг моҳияти, унга қарши кураш, муаммолар, ечимлар ҳақида сўз боради. Дунё бўйича кузатилаётган ҳолат, Ўзбекистонда кибержиноятга қарши қилинаётган саъй-ҳаракатлар, ҳуқуқий масалалар, бажарилиши лозим бўлган ишлар ёритилади.*

Калит сўзлар: *кибержиноят, кодекс, муаммо, интернет, компьютер, дастур.*

Аннотация. *В статье рассматриваются понятия цифровых технологий, киберпространство, киберпреступность, ее сущность, борьба с ней, проблемы и пути их решения. Освещаются ситуация в мире, усилия Узбекистана по борьбе с киберпреступностью, правовые вопросы, работы, которые необходимо предстоит сделать.*

Ключевые слова: *киберпреступность, кодекс, проблема, интернет, компьютер, программа.*

Annotation: *The article deals with the concept of digital technology, cyberspace, cybercrime, its essence, the fight against it, problems, solutions. The current situation in the world, the efforts being made in Uzbekistan against cybercrime, legal issues, the work to be done will be covered.*

Keywords: *cybercrime, code, problem, internet, computer, software.*

КИРИШ.

Рақамли технологиялар соҳасидаги ҳуқуқбузарликлар тараққий этган жамиятдаги жиноятнинг бир тури ҳисобланади. Жамият тараққий топиши билан жиноят турлари ҳам ўзгариб бораверади. Бугунги кунда вояга етган деярли ҳар бир инсон интернет ресурсларидан фойдаланади. Бу жараён эса ўзига хос хавф-хатарга эга, яъни кибержиноят қурбонига айланиш ҳеч гап эмас. Кибержиноятнинг кўплаб турлари мавжуд бўлиб, у нафақат жисмоний шахсга қаратилган бўлиши, балки улкан давлат миқёсидаги моддий ва маънавий бойликлар талон-тарожига қаратилган бўлиши ҳам мумкин. Шу боисдан давлатимизда қонун лойиҳалари қайта кўриб чиқилмоқда.

АДАБИЁТЛАР ШАРҲИ

Жумладан, Ўзбекистон Республикаси Президентининг 2018 йил 14 майдаги “Жиноят ва жиноят-процессуал қонунчилиги тизимини тубдан такомиллаштириш чора-тадбирлари тўғрисида”ги ПҚ–3723-сонли қарорида “Технологик тараққиёт, жумладан кибержиноят билан боғлиқ жиноят турларининг кенгайганлигини ҳисобга олган ҳолда ахборот технологиялари соҳасида жавобгарликни назарда тутувчи нормаларни қайта кўриб чиқиш” назарда тутилган [1]. Ундан ташқари Ўзбекистон Республикаси Жиноят кодексининг 278^5-моддасига кўра, ўзганинг компьютер ускунасини қасддан ишдан чиқариш, худди шунингдек, компьютер тизимини бузиш (компьютер саботажи):

– 3 йилгача муайян ҳуқуқдан маҳрум қилиб, 66 млн. 900 минг сўмдан 89 млн. 200 минг сўмгача миқдорда жарима;

– 2 йилгача озодликни чеклаш;

– 2 йилгача озодликдан маҳрум қилиш билан жазоланади.

– шунингдек, мазкур ҳаракатларни гуруҳ бўлиб, такроран ёки хавфли рецидивист томонидан содир етиш 3 йилгача озодликдан маҳрум қилиш билан жазолашга сабаб бўлиши мумкин [2].

Кибержиноятлар ахборот технологиялари соҳасидаги жамоатчилик муносабатларига жиддий таҳдид солади ва шунинг учун замонавий шароитда уларга қарши курашиш давлат ва фуқаролар учун жиддий муаммога айланди. Давлатнинг ҳуқуқни муҳофаза қилиш органлари уларни зарарсизлантириш бўйича қарши чораларни, кибержиноятларга қарши курашиш стратегияси ва тактикасини ишлаб чиқмоқда [3].

Кибержиноятлар муайян шароитларда содир этилади, уларнинг содир этилишига ёрдам берадиган омиллар мавжуд. Уларни аниқлаш ва

илмий таҳлил асосида суд экспертиза усулини, тегишли тергов ҳаракатларини ўтказиш тактикасини ишлаб чиқиш керак [4].

Кибермаконда содир етилган ушбу жиноятларга компьютерлар, компьютер дастурлари, компьютер тармоқлари фаолиятига қонунга хилоф равишда аралашиш, компьютер маълумотларига рухсатсиз кириш, нусха олиш, ўзгартириш, шунингдек, ахборот-коммуникация технологиялари, компьютер тармоқлари ёрдамида ёки улар орқали содир этилган бошқа ноқонуний ижтимоий хавфли ҳаракатлар киради.

ТАДҚИҚОТ МЕТОДОЛОГИЯСИ ВА ЭМПИРИК ТАҲЛИЛ

Эҳтимол, кибертаҳдид манбалари нафақат хакерлар ёки уларнинг гуруҳлари, балки алоҳида давлатлар, террорчилик, жиноий гуруҳлар ҳам ҳисобланади. Кибержиноятларга қарши курашиш воситалари ва усулларини ишлаб чиқишда жиноятнинг латентлик даражасидан хабардор бўлиш керак. Мутахассислар тахминига кўра, “компьютер жинояти”нинг латентлиги АҚШда 80% га, Буюк Британияда – 85% га, Германияда – 75% га, Россияда – 90%га кўпроқдир[5]. “Symantec Security” халқаро киберхавфсизлик хизмати маълумотларига кўра, “ҳар сонияда” дунё бўйлаб, 12 нафар киши киберҳужумга учрайди ва дунёда ҳар йили тахминан 556 млн. кибержиноятлар содир этилади ва бунинг натижасида 100 миллиард АҚШ долларидан зиёд зарар етказилади [6].

Масалан, Қўшма Штатларда аллақачон фаолият кўрсатаётган Миллий киберхавфсизлик маркази билан бир қаторда Қуролли Кучлар Бирлашган кибер Қўмондонлиги ҳарбий ҳаракатларни амалга ошириш пайтида Пентагон тузилмалари тегишли ёрдамни тақдим этади. Бу глобал миқёсда барчанинг саъй-ҳаракатларини мувофиқлаштириб боради. Фуқаролик федерал институтлари ва шунга ўхшаш дастурий таъминот билан ўзаро алоқададир [7]. Шу билан бирга, ушбу ташкилотлар қисман назорат қилинадиган бўлимлардир, чунки « назорат қилувчи тузилма “Кенгашдир”. Миллий хавфсизлик соҳасидаги қўмиталар ахборот стратегиясини амалга оширишни ўз ичига олади [8]. Киберқурол дастурлари Буюк Британияда расмийларнинг киберкосмосдан келиб чиқадиган таҳдидларга қарши туриш қобилиятини таъминлашда амалга оширилади [9]. Австралияда электрон почта хавфсизлигини мувофиқлаштириш гуруҳи ташкил этилган бўлиб, ушбу гуруҳнинг асосий вазифаси ҳам давлат, ҳам хусусий сектор учун операцион маконда ишончли ҳимоя электрон тизимини яратишдир. Кибержиноятларнинг олдини олиш бўйича тадбирлар нафақат алоҳида давлатлар томонидан амалга оширилади, балки уларнинг блоклари, хусусан, НАТО томонидан амалга оширилиб келинмоқда. Шундай қилиб, сўнгги йилларда қабул қилинган барча блок-йўриқнома ҳужжатлари ушбу муаммонинг аҳамиятини кўрсатиб беради. Стратегик жиҳатдан биринчи марта НАТО концепциясида альянс фаолиятида қоидалар киритилган бўлиб, ҳарбий соҳанинг янги йўналиши сифатида кибермайдон пайдо бўлган [10].

НАТИЖАЛАР

Бизнинг юртимизда ҳам сўнгги пайтларда бир қатор кибержиноятлар кузатилмоқда.

Хусусан, Самарқанд вилоятида бир гуруҳ шахслар томонидан “OLTINYUL.UZ” ва “E-SUM.UZ” веб-сайтлари орқали фуқароларни мулкий манфаатга қизиқтириб, “Молиявий пирамида” лойиҳаси тузилган.

Шу асосда 8 200 нафардан зиёд фуқародан жами 450 млн. сўмдан ортиқ пул маблағлари йиғилиб, ушбу гуруҳ томонидан ўзлаштирилган.

Ҳолат юзасидан ИИВ ҳузуридаги Тергов департаменти томонидан Н.Р. ва унинг шерикларига нисбатан Ўзбекистон Республикаси Жиноят кодексининг 188(1)-моддаси 2-қисми билан жиноят иши қўзғатилган.

Бундан ташқари, 2018 йил 23 июль куни Тошкент шаҳрида 5 та автотранспорт воситасининг давлат рақамлари ўғирланиб, жабрланувчилардан давлат рақамларини қайтариш эвазига Интернет тармоғидаги “QIWI” ва “WEB money” электрон тизимлари орқали пул талаб қилинган. Кўрилган чоралар натижасида ушбу жиноятни Тошкент шаҳар Бектемир туманида яшовчи 19 ёшли фуқаро содир этганлиги аниқланиб, қўлга олинган.

Шунингдек, 2018 йилнинг 4 октабрь куни Интернет тармоғининг “Telegram” мессенжеридаги 374 мингдан ортиқ аъзолари бўлган каналдан телефон ва компьютер воситаларига зарар келтирувчи дастурлар тарқатилган. Кўрилган чоралар натижасида ушбу жиноятни Фарғона вилоятида яшовчи М.В. содир этганлиги аниқланиб, қўлга олинган [11].

Кибержиноятчиликка қарши Будапешт конвенцияси 2001 йил 23 ноябрь Интернет ва компьютер жинояти (кибержиноят)ларни уйғунлаштириш орқали миллий қонунлар, тергов усулларини такомиллаштириш ва халқлар ўртасидаги ҳамкорликни ошириш юзасидан имзоланган.

2006 йил 1 мартда Кибержиноятчилик тўғрисидаги конвецияга қўшимча протокол кучга кирди. Қўшимча протоколни ратификация қилган давлатлар ирқчи ва ксенофобик компьютер тизимлари орқали материал, шунингдек, ирқчилик ёки ксенофобия томонидан таҳдид ва ҳақорат тарқатишни жиноий жавобгарликка тортишлари шартлиги белгиланди [12].

Конвенция интернет ва бошқа компьютер тармоқлари орқали содир этилган жиноятлар бўйича биринчи халқаро шартномадир, у хусусан, муаллифлик ҳуқуқининг бузилиши, компьютер билан боғлиқ фирибгарлик, болалар порнографияси, таҳдид жиноятлари ва тармоқ хавфсизлиги жиноятларини ўз ичига олади. Шунингдек, у компьютер тармоқларини қидириш ва қонуний ушлашга доир қатор ваколатлар ва процедураларни ўз ичига олади. Унинг муқаддимасида келтирилган асосий мақсади жамиятни ҳимоя қилишга қаратилган умумий жиноят сиёсатини олиб боришдир. Шунингдек, кибержиноятларга доир тегишли қонунларни қабул қилиш ва жорий этиш орқали халқаро ҳамкорликни тарғиб этади.

Конвенция, асосан:

– кибержиноятчилик соҳасидаги ҳуқуқбузарликлар ва улар билан боғлиқ қоидаларни ички жиноят моддий-ҳуқуқий элементларини уйғунлаштириш;

– ички жиноят-процессуал қонунчилигини тергов қилиш ва жиноий жавобгарликка тортиш учун зарур бўлган ваколатларни, шунингдек, электрон тизимда бўлган компьютер тизими ёки далиллар ёрдамида содир этилган бошқа ҳуқуқбузарликларни таъминлаш;

– халқаро ҳамкорликнинг тезкор ва самарали режимини ўрнатишга қаратилган.

Конвенция томонидан қуйидаги ҳуқуқбузарликлар белгиланган: ноқонуний кириш, ноқонуний йўл билан тутиш, маълумотларга аралашиш, тизимга аралашиш, қурилмалардан нотўғри фойдаланиш, компьютер билан боғлиқ қалбакилаштириш, компьютер билан боғлиқ фирибгарлик, болалар порнографияси ва муаллифлик ҳуқуқи ва турдош ҳуқуқлар билан боғлиқ ҳуқуқбузарликлардир [13].

Дарҳақиқат, кўришимиз мумкинки, бутун дунё ушбу турдаги жиноятларга қарши курашаётган бир даврда МДҲ мамлакатлари ҳам бундан четда турмади. 2018 йил 28 сентябрда кибержиноятларни тергов қилишда ҳамкорлик қилиш масаласини тартибга солувчи ихтисослаштирилган ҳужжатлардан бири ҳисобланмиш Мустақил Давлатлар Ҳамдўстлигига аъзо давлатлар ўртасида ахборот технологиялари соҳасида жиноятларга қарши курашиш бўйича Битим имзоланди. Озарбайжон Республикаси, Арманистон Республикаси, Белорусия, Қозоғистон Республикаси, Қирғизистон Республикаси, Россия Федерацияси, Молдова Республикаси, Тожикистон Республикаси, Туркманистон Республикаси, Ўзбекистон Республикаси ва Украина ушбу Битим қатнашчилари ҳисобланади. Ўзбекистон Республикаси Президентининг 13.02.2019 йилдаги ПҚ–4188-сонли қарори билан 2018 йил 28 сентябрда МДҲ давлатлари раҳбарлари кенгашининг мажлисида имзоланган Мустақил Давлатлар Ҳамдўстлигига аъзо давлатлар ўртасида ахборот технологиялари соҳасидаги жиноятларга қарши курашиш соҳасида ҳамкорлик тўғрисидаги Битим тасдиқланди. Ушбу Битимни амалга ошириш бўйича ваколатли органлар сифатида *Ўзбекистон Республикаси Ички ишлар вазирлиги, Давлат хавфсизлик хизмати ва Ахборотлаштириш ва телекоммуникациялар соҳасида назорат бўйича давлат инспекцияси* белгиланди.

Қонунчилигимизда компьютер ахбороти соҳасидаги жиноий ҳаракатлар, маълумки, Ўзбекистон Республикасининг Жиноят кодекси XXI боби (“Ахборот технологиялари соҳасидаги жиноятлар”(2781–2787-моддалар)да ўз аксини топган. Ушбу жиноятларнинг хусусиятлари ахборот-коммуникация технологияларидан қонунга хилоф равишда фойдаланиш билан боғлиқ ижтимоий хавфли қилмишларнинг кичик бир қисмига тааллуқлидир. Қайд этиш жоизки, Ўзбекистон Республикаси

Жиноят кодексида унга берилган изоҳларда ахборотни тўплаш ва тарқатишнинг ахборот-коммуникация усуллари ва воситаларидан фойдаланиш масалалари батафсил ўз аксини топмаган. DDos ҳужумлари, фишинг ва кибержиноятларни содир этишнинг бошқа воситалари ва усулларидан фойдаланиш, айниқса, интернет-банкинг Ўзбекистон Республикаси Жиноят кодексида алоҳида акс эттирилмаган. Ҳозирги вақтда жиноят қонунчилиги олдида кибержиноятларга қарши курашиш соҳасидаги қонунчиликни ўз вақтида такомиллаштириш зарурати билан боғлиқ вазифалар турибди.

ХУЛОСА ВА МУНОЗАРА

Мамлакатимиз Жиноят кодексининг ахборот технологиялари соҳасига оид еттинчи моддасида ва бошқа қонун ҳужжатларида ахборот тизимлари, интернет тармоғидаги ахборотдан фойдаланувчилар, провайдерлар, оммавий ахборот воситаларининг ва бошқаларнинг жавобгарлиги тўғрисидаги айрим қоидалар етишмайди. Шу сабабли Ўзбекистон Республикаси Жиноят кодексига ўзгартиришлар (ўзгартириш ва қўшимчалар)ни ишлаб чиқиш ва белгиланган тартибда киритишнинг реал зарурати вужудга келди. Жиноят кодексига ўзганинг мулкини ўғирлаш (ўғирлик, фирибгарлик, товламачилик), алоқа тармоқлари, шу жумладан, интернет билан боғлиқ жиноятларни тартибга солиш бўйича ахборот тизими ва маълумотларга рухсатсиз кириш, пластик ва кредит карталар орқали пул маблағларини ечиб олиш билан боғлиқ маълумотларни қўшиб, ўзгартириш ва қўшимчалар киритиш мақсадга мувофиқ, деб ҳисоблаймиз.

Замонавий воқеликни ҳисобга олган ҳолда «кибержиноят»нинг комплекс тушунчасини белгилаш учун ушбу жиноятларнинг асосий элементларини аниқлаш бўйича илмий тадқиқотлар олиб бориш ва ушбу ижтимоий хавфли қилмишларни тергов қилиш методологиясини ишлаб чиқиш давр талабидир.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР РЎЙХАТИ:

1. www.lex.uz.
2. www.norma.uz.
3. Карпова Д.Н. Киберпреступность: глобальная проблема и еѐ решение. // Власть. №8. – 2014. – Б. 46–50.
4. Анорбоев А.У Кибержиноятчилик, унга қарши курашиш муаммолари ва киберхавфсизликни таъминлаш истиқболлари. Монография – Т.: Миллий гвардия институти, 2020. – Б. 324.
5. Salayev N.S., Ro‘ziyev R.N Kiberjinoyatchilikka qarshi kurashishga oid milliy va xalqaro standartlar. Monografiya., – T.: TDYU, 2018. – B. 139.
6. Karpova D.N. Sybersrimes: a global issuye and its solution. Vlast’= The Pover No. 8. – B. 46–50. (In Russian).

7. Berd k. A var vith many unknovn quantitiyes. Somputerra, 2009, No. 20, B. 26–29. (In Russian)

8. Zav'yalov S. International yexperiyense in fighting the propaganda of terrorism in The Internet. Zarubezhnoyevoyennoyeobozreniye = Foreign Military Reviyev, 2014, No. 4. – B. 34–39. (In Russian).

9. Khims'henko I.A. Informatsionnoyeobshs'hestvo: pravoveproblemy v usloviyakhglobalizatsii. Kand. Diss. [Information sosiyety: legal basis in the sonditions of globalization. Sand. Diss.]. Mossov, 2014. – B. 174.

10. Gradov A. The astivitiyes of The North Atlantis Treaty Organization in the sphere of syber-sesurity. Zarubezhnoyevoyennoyeobozreniye = Foreign Military Reviyev, 2014, No. 7. B. 13–16. (In Russian).

11. https://advokatnews.uz/.

12. http://indianexpress.com/article/india/home-ministry-pitches-for-budapest-convention-on-cyber security-rajnath-singh-5029314/.

13. Convention on cybercrime, opening of the treaty: Budapest, 23/11/2001. URL: www.coe.int/en/web/cybercrime/the- budapest-convention.