O‘ZBEKISTON RESPUBLIKASI
KRIMINOLOGIYA TADQIQOT INSTITUTI

KRIMINOLOGIYA YANGILIKLARI

Ilmiy to‘plam

Toshkent – 2026

O‘zbekiston Respublikasi Kriminologiya tadqiqot instituti kengashining yig‘ilishida muhokama qilingan hamda nashrga tavsiya etilgan.

Mas’ul muharrir

O‘zbekiston Respublikasi Kriminologiya tadqiqot instituti boshlig‘i, yuridik fanlar bo‘yicha falsafa doktori (PhD) **B.E.Berdialiyev.**

Taqrizchilar:

siyosiy fanlar doktori, professor **I. Ergashev;**

yuridik fanlar doktori, professor **A.G. Zakirova**

Nashrga tayyorlovchilar:

falsafa doktori (PhD), professor **R.O.Nigmatov;** yuridik fanlar bo‘yicha falsafa doktori (PhD) **Sh.O. Azim;** tibbiyot fanlari bo‘yicha falsafa doktori (PhD) **I.E. To‘raev;** falsafa fanlari bo‘yicha falsafa doktori (PhD), dotsent **Sh.Sh. Hasanov;** yuridik fanlari bo‘yicha falsafa doktori (PhD) **U.A. Irisbekov; D.B.Mamarajabova.**

Kriminologiya yangiliklari: Ilmiy to‘plam / Mas’ul muharrir yuridik fanlar bo‘yicha falsafa doktori (PhD) B.E.Berdialiyev – T.: O‘zbekiston Respublikasi Kriminologiya tadqiqot instituti, 2026. – 168 b.

Mazkur to‘plamda zamonaviy kriminologiya nuqtai nazaridan jinoyatchilikka qarshi kurashning dolzarb masalalari yoritilgan bo‘lib, sodir etilayotgan jinoyatlarning kriminologik tavsifi, ularning kelib chiqish omillari, jinoyatchilikning oldini olish va fosh etishda yuzaga kelayotgan muammolar, shuningdek, xorijiy davlatlarning ilg‘or tajribalari va ularni milliy amaliyotga tatbiq etish imkoniyatlari ilmiy va amaliy jihatdan tahlil qilingan.

To‘plam huquq-tartibot organlari ta’lim muassasalarining professor-o‘qituvchilari, olimlar, tadqiqotchilar va amaliyot xodimlari, mustaqil izlanuvchilar, talabalar hamda kursantlar uchun mo‘ljallangan.

© O‘zbekiston Respublikasi Kriminologiya tadqiqot instituti, 2026-y.

КИБЕРХАВФСИЗЛИКНИНГ ПРОФИЛАКТИКАСИ ТЎҒРИСИДА АЙРИМ МУЛОҲАЗАЛАР

Ҳасанов Шарофиддин Шамшурович
Ўзбекистон Республикаси Криминология тадқиқот институти етакчи илмий ходими, фалсафа фанлар бўйича фалсафа доктори (PhD), доцент

Аннотация. Мақолада киберхавфсизлик ва кибержиноятлар соҳасини тартибга солишга нисбатан ягона ёндашув, маълумотларга ишлов бериш ҳамда уларни ҳимоя қилиш бўйича дастурий ва техник воситаларни ишлаб чиқиш, жорий этиш жараёнини ташкил этиш, мониторинги ва назоратини амалга оширишга қаратилган ахборот тизимлари ҳамда ресурсларини киберхавфсизлик бўйича ягона давлат тизими жорий этилган ҳолда таъминланиши бўйича мазкур масала тартибга солинишининг таҳлили сифатида ёритилган ва тавсифланган.

Калит сўзлар: кибержиноят, хакерлик жинояти, зарарли дастурларни яратиш, сақлаш ва тарқатиш, компьютер фирибгарлиги, шахсий маълумотларни ўғирлаш, кетфишинг, фрейпинг, киберсквоттин, компьютер маълумотлари мазмунига оид ҳуқуқбузарликлар.

Аннотация. В статье рассмотрен и описан единый подход к регулированию сферы кибербезопасности и киберпреступлений, разработка программного обеспечения и технических средств обработки данных и их защиты, организация, мониторинг и контроль процесса внедрения, мониторинг и контроль информационных систем и ресурсов. Также проводится анализ регулирования данной проблемы с введением единой государственной системы кибербезопасности.

Ключевые слова: Киберпреступления, хакерские преступления, создание, хранение и распространение вредоносного программного обеспечения, компьютерное мошенничество, кража личных данных, ловля рыбы, мошенничество, киберсквоттинг, нарушения содержания компьютерных данных.

Abstract. A unified approach to the regulation of cyber security and cyber crimes, a unified state system for combating cyber security and cyber crimes, aimed at organizing, monitoring and controlling the process of developing and implementing software and technical tools for data processing and their protection, has been introduced. This issue is covered and described as an analysis of regulation.

Keywords: Cybercrimes, hacker crimes, creation, storage and distribution of malicious software, computer fraud, identity theft, fishing, fraud, cybersquatting, computer data breaches.

Дунёда киберхавфсизликни таъминлаш ва кибержиноятларга қарши курашиш борасида *“рақамли иқтисодиёт”*ни *ривожлантириш ва ахборот-телекоммуникация технологиялар соҳаси тараққиётига алоҳида эътибор қаратилмоқда. Хусусан,* киберхавфсизлик ва кибержиноятлар соҳаларига оид тегишли чораларни кўриш, улар борасида профилактик тадбирларни самарали қўллаш *бўйича тизимли ишлар олиб борилмоқда.*

Шу ўринда Ўзбекистон Республикасида ҳам ахборотлаштириш ва Интернет тармоғини ривожлантириш ишлари кенг амалга оширилган. Бунда Ўзбекистон мустақилликка эришган вақтда, яъни 1991 йили фақатгина электрон почта учун биринчи маълумотларни узатиш тизимига кириш имконияти пайдо бўлган. 1992–1995 йилларга келиб эса, илк локал провайдерлар иш бошлаган.

1995 йилнинг 29 апрель куни “UZ” домени ишга тушган. 1995–2000 йиллар Интернет тармоғи мамлакат доирасида катта тезликда ривожланиш босқичини босиб ўтган ва ҳозирги кўринишга келган[1].

Мамлакатимизда киберхавфсизликка оид муаммолар, *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 ана шу мақсадга хизмат қилмоқда. Шу билан бир қаторда, шахсларни Интернет ҳамлаларидан ҳимоялаш, ахборот олиш ва тарқатиш маданиятини тарғиб қилиш, тармоқ хавфсизлигини таъминлаш юзасидан чора-тадбирлар амалга оширилмоқда. Оммавий ахборот воситалари орқали мунтазам равишда Интернет тармоқларидан фойдаланиш қоидалари,* веб-*макондаги хавф ва фирибгарликларга қарши курашиш усуллари тушунтирилмоқда.*

Ушбу ўзгаришлар ҳаёт сифатини яхшилаш билан бир қаторда, жиноятчиликнинг янги шакли киберхавфсизликни таъминлаш ва кибержиноятлар*ни юзага келишига замин яратди ҳамда ҳаётимизга “киберхавфсизлик”, “кибержиноятчилик” тушунчасини олиб кирди. Интернет билан боғлиқ киберхавфсизликни таъминлаш бўйича халқаро* Symantec Security *ташкилотининг маълумотларига кўра, ҳозирда ҳар сонияда дунёдаги 12 нафар инсондан биттаси Интернет ҳужум қурбони бўлмоқда ва ҳар йили 556 млн.* дан *кўпроқ киберҳужум уюштирилади ва бунда жабрланувчилар кўрадиган зарар миқдори 100 млрд.* АҚШ *долларидан кўпроқдир[2] .*

*Жаҳонда “Глобал ахборотлаштириш ва компьютерлаштириш асри”*да *инсоният ҳаётида оламшумул ихтиролар билан бир қаторда, ахборот хавфсизлигига таҳдид солаётган Интернет тармоқларидан фойдаланиб содир этилаётган жиноятларни жиноят-ҳуқуқий ва криминологик жиҳатларини аниқлаш, динамикасини таҳлил қилиш ҳамда ушбу турдаги жиноятчиликнинг*

сабаб ва шароитлари, жиноятчи шахсини ўрганиш ва уларни олдини олиш бўйича таклифларни ишлаб чиқиш муҳим аҳамият касб этмоқда.

Ўзбекистон Республикаси Президентининг 2019 йил 14 сентябрдаги ПҚ-4452-сон “Ахборот технологиялари ва коммуникацияларининг жорий этилишини назорат қилиш, уларни ҳимоя қилиш тизимини такомиллаштиришга оид қўшимча чора-тадбирлар тўғрисида”ги қарори асосан киберхавфсизлик, уни тартибга солиш соҳасида ваколатли орган Ўзбекистон Республикаси Давлат хавфсизлик хизмати ҳисобланади. Ўз навбатида, Ўзбекистон Республикаси Ахборотлаштириш ва телекоммуникациялар соҳасидаги назорат бўйича давлат инспекцияси “Киберхавфсизлик маркази” давлат унитар корхонаси билан биргаликда давлат ва хўжалик бошқаруви органларида маҳаллий давлат ҳокимияти органларида бошқа ташкилотлар ва идораларда ахборот-коммуникация технологияларини жорий этиш ва ривожлантириш, ахборот хавфсизлиги ҳолатини назорат қилиш, мониторинг қилиш, ўрганиш ва текширишни амалга оширади.

Бундан ташқари, рақамли маълумотлар хавфсизлиги билан боғлиқ хавфларнинг ортиб бориши, давлат ва жамият манфаатлари ҳамда фуқароларнинг шахсий ҳуқуқларига таҳдид солиши – глобал рақамли бошқарув учун янги муаммоларни келтириб чиқараётганлиги сабабли жорий йилнинг 15 март куни “Киберхавфсизлик тўғрисида”ги қонун президент томонидан имзоланди[3]. Ҳужжатга кўра, Ўзбекистонда киберхавфсизлик соҳасидаги ягона давлат сиёсатини президент белгилайди (10-модда), Давлат хавфсизлик хизмати эса киберхавфсизлик соҳасидаги ваколатли давлат органи ҳисобланади.

Киберхавфсизликни таъминлашдаги асосий принциплари қонунийлик, шахс ва давлат манфаатларини ҳимоя қилиш, соҳага ягона ёндашув, тизимни яратишда (давлат харидларида) маҳаллий ишлаб чиқарувчиларга устуворлик бериш, халқаро ҳамкорлик учун очиқлик ҳисобланади. (4-модда)

Ушбу қонунда ҳам, бошқа кўплаб ҳужжатлар каби Ўзбекистон қўшилган халқаро шартномаларда кўзда тутилган бошқача қоидаларда устуворлик берилган. Яъни, халқаро шартномада “Киберхавфсизлик тўғрисида”ги қонундан бошқача қоида назарда тутилган бўлса, халқаро шартнома қоидалари қўлланилади. (2-модда)

Киберхавфсизлик соҳасидаги ваколатли орган – ДХХга кўплаб ваколатлар берилган, хусусан:

соҳага доир норматив ҳужжатлар ва дастурлар ишлаб чиқиш, уларнинг ижросини назорат қилиш;

киберхавфсизлик ҳодисалари юзасидан тезкор тадбирлар ва тергов ҳаракатлари олиб бориш**,** шунингдек, уларнинг олдини олиш, бартараф қилиш ва оқибатларини тугатиш бўйича техник чоралар кўриш;

соҳага доир тадқиқотлар ва мониторинглар ўтказиш;

муҳим ахборот инфратузилмалари объектларининг ягона реестрини шакллантириш, уларнинг хавфсизлигини таъминлашга доир талабларни белгилаш;

ахборотни криптографик ҳимоя қилиш воситаларини ишлаб чиқишга доир фаолиятни лицензиялаш;

муҳим ахборот инфратузилма объектларига киберҳужумларга уринишларнинг олдини олиш;

давлат бошқарув органлари ва маҳаллий ҳокимликларни кибертаҳдидлар ҳақида огоҳлантириш;

Ўзбекистон кибермаконида террорчилик, экстремистик ва бошқа қонунга хилоф фаолият олиб борилмаслиги чораларини кўриш;

киберхавфсизлик соҳасида кадрларни тайёрлаш ва бошқа кўплаб ваколатларга эга[4].

Соҳа бўйича ваколатли орган – ДХХнинг қонуний талаб ва кўрсатмаларини бажариш мажбурийдир (11-модда).

Шунингдек, ваколатли орган қуйидаги ҳуқуқларга эга:

киберҳужумларни аниқлаш ва бартараф этишда техник, дастурий воситаларни ижарага олиш;

кечиктириб бўлмайдиган чоралар кўриш учун техник қурилмалар ва хизматлардан текин фойдаланиш**;**

давлат органлари ва ташкилотларига кириш, улардан зарур ҳужжатлар ва материалларни олиш ва фойдаланиш;

текширув ва назоратни амалга ошириш учун давлат ташкилотлари, муҳим ахборот инфратузилмалари объектларининг ахборот тизимлари ва ресурсларига тўсқинликсиз кириш**;**

жисмоний ва юридик шахсларнинг турар жойларига ва бошқа объектларига тўсқинликсиз кириш, зарурат бўлганда қулфлаш мосламаларини бузиш, шунингдек, жиноят содир этиб таъқиб қилинаётган ёки шундай жиноят содир этаётган шахс бор деб ҳисоблаш учун етарли асослар бўлса ёхуд кечиктириш фуқаролар ҳаётини таҳдидга қўйса, бу жойларни кўздан кечириш (етказилган зарарни қоплаш ва 24 соат ичида прокурорга хабар бериш шарти билан) ва бошқалар (12-модда).

ДХХ киберхавфсизлик соҳасидаги муаммолар юзасидан илмий-тадқиқотлар амалга ошириш, соҳага доир ҳуқуқбузарликлар тўғрисидаги мурожаатлар ва маълумотларни рўйхатдан ўтказиш ва чора кўриш каби мажбуриятларга эга (13-модда).

Давлат органлари ва ташкилотлари ҳам киберхавфсизликни таъминлаш мақсадида ваколатли давлат органидан кибертаҳдидлар, дастурий таъминотдаги, ускуналар ва технологиялардаги заифликлар тўғрисидаги ахборот ва маслаҳатлар олиш ҳуқуқига эга. Шунингдек, давлат органлари ва ташкилотлари ваколатли органни киберҳужумлар тўғрисида огоҳлантириши, киберҳимоя учун сертификатлаштирилган дастурий таъминотлардан фойдаланиши, соҳага доир норматив ва техник ҳужжатларни ваколатли орган билан келишиши шарт. (14-модда).

Давлат органлари ва ташкилотларининг ахборот тизимлари ҳамда ресурслари маълумотларининг сақланишини таъминлаш маълумотларнинг захира нусхаларини яратиш йўли билан амалга оширилади, уларнинг сақланиш муддати охирги 3 ойдан кам бўлмаслиги керак (15-модда).

Муҳим ахборот инфратузилмаси объектлари ва миллий ахборот ресурсларидан фойдаланиш билан боғлиқ муайян ҳуқуқларга эга юридик шахслар, яъни киберхавфсизлик субъектларига ҳам ушбу қонун доирасида бир қанча ҳуқуқ ва мажбуриятлар юклатилган (16-модда).

Киберхавфсизлик талабларига мувофиқлик юзасидан экспертиза мажбурий тартибда ёки киберхавфсизлик субъектларининг ташаббусига кўра амалга оширилади. Қуйидагилар киберхавфсизлик талабларига мувофиқлик юзасидан мажбурий тартибда экспертизадан ўтказилиши лозим (18-модда):

давлат органларининг ахборот ресурслари;

давлат органларининг ахборот тизимлари;

муҳим ахборот инфратузилмаси объектлари тоифасига киритилган ахборот тизимлари.

Шунингдек, давлат органлари ва ташкилотлари ахборот тизимлари ҳамда ресурсларининг киберхавфсизлигини таъминлаш учун қўлланиладиган аппарат, аппарат-дастурий ва дастурий воситалар мажбурий тартибда сертификатлаштирилиши лозим (19-модда).

Киберхавфсизлик ҳодисалари ваколатли давлат органи ёки киберхавфсизликни таъминлаш бўйича ишчи органнинг мансабдор шахслари томонидан текширилади. Шунингдек, техник имкониятларга эга бўлса ахборот ресурсининг ўзи ҳам текширув ўтказиши мумкин. Бунда у ваколатли органни натижалардан хабардор қилиши керак (22-модда).

Шунингдек, қонуннинг олтинчи бобида муҳим ахборот инфратузилмаси объектларининг киберхавфсизлигини таъминлаш, уларни тоифалаштириш ва реестрини юритиш, ҳуқуқ ва мажбуриятлари ҳамда хавфсизлик талабларига доир нормалар берилган (25-31 моддалар).

Ҳужжатнинг еттинчи бобидан соҳани қўллаб-қувватлаш ва ривожлантиришга доир нормалар ўрин олган. Хусусан, соҳага доир норматив-ҳуқуқий базани такомиллаштирилиб, киберхавфсизлик субъектларини давлат томонидан қўллаб-қувватлаш доирасида уларга солиқ, божхона имтиёзлари ва преференциялар берилиши, хўжалик юритувчи субъектларнинг маблағларини соҳани молиялаштириш учун жалб қилишга шароит яратиш белгиланган. (32-модда).

Давлат хавфсизлик хизмати Ўзбекистон қонунчилиги ва халқаро шартномаларига мувофиқ, халқаро кибержиноятчиликка қарши курашиш масалаларига доир ахборотни чет давлатларга ва халқаро ташкилотларга сўров бўйича тақдим қилади. Агар бундай ахборот тергов ва суд жараёнларига тўсқинлик қилмаса ҳамда киберҳужумларга барҳам беришга хизмат қилса,

ваколатли орган уни хорижий давлатлар ва халқаро ташкилотларга олдиндан сўровсиз ҳам бериши мумкин. (36-модда).

Хўш, “кибержиноятчилик” тушунчасининг ўзи нима эканлиги, унинг таркибий қисмлари ҳамда биз сўнгги пайтларда тез-тез учратишга одатланиб қолган кибермаконга оид ибораларга тўхталиб ўтамиз:

Киберхавфсизлик – 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 [5].

Кибержиноятчилик тушунчаси ахборот-коммуникация технологиялари соҳасидаги кўплаб турдаги жиноятларни ўзида бирлаштирган. Виртуал тармоқда даҳшат солиш, вирус ва бошқа зарарли дастурлар, қонунга зид ахборотлар тайёрлаш ва тарқатиш, электрон хатларни оммавий тарқатиш (спам), хакерлик ҳужуми, веб-сайтларга ноқонуний кириш, фирибгарлик, муаллифлик ҳуқуқини бузиш, кредит карточкалари рақами ва банк реквизитларини ўғирлаш (фишинг ва фарминг) ҳамда бошқа турли ҳуқуқбузарликлар шулар жумласидандир. Бундай ҳолатларда жиноятчилар ўзларини қизиқтирган “объектлар”га моддий ва маънавий зарар етказишни ўз олдига мақсад қилиб қўяди. Кибержиноятчилик ва уни содир этувчи кимсалар доираси эса йилдан йилга кенгайиб бораётганини ҳаётнинг ўзи кўрсатиб турибди [6];

Кибержиноятчиликка доир тушунчаларни қўйдагича тавсифлаш мумкин:

Кибермакон – ахборот технологиялари ёрдамида яратилган виртуал муҳит.

Кибертаҳдид – кибермаконда шахс, жамият ва давлат манфаатларига таҳдид солувчи шарт-шароитлар ва омиллар мажмуи.

Киберхавфсизлик – кибермаконда шахс, жамият ва давлат манфаатларининг ташқи ва ички таҳдидлардан ҳимояланганлик ҳолати.

Киберхавфсизлик ҳодисаси – кибермаконда ахборот тизимларининг ишлашида узилишларга ва (ёки) улардаги ахборотнинг очиқлиги, яхлитлиги ва ундан эркин фойдаланилишининг бузилишига олиб келган ҳодиса.

Киберхавфсизлик объекти – ахборотнинг киберҳимоя қилинишини ҳамда миллий ахборот тизимлари ва ресурсларининг киберхавфсизлигини таъминлашга доир фаолиятда фойдаланиладиган ахборот тизимлари мажмуи, шу жумладан муҳим ахборот инфратузилмаси объектлари.

Киберхавфсизлик субъекти – миллий ахборот ресурсларига эга бўлиш, улардан фойдаланиш ва уларни тасарруф этиш ҳамда улардан фойдаланиш бўйича электрон ахборот хизматлари кўрсатиш, ахборотни ҳимоя қилиш ҳамда киберхавфсизлик билан боғлиқ муайян ҳуқуқлар ва мажбуриятларга эга бўлган юридик шахс ва (ёки) якка тартибдаги тадбиркор, шу жумладан муҳим ахборот инфратузилмаси субъектлари.

Киберҳимоя – киберхавфсизлик ҳодисаларининг олдини олишга, киберҳужумларни аниқлашга ва улардан ҳимоя қилишга, киберҳужумларнинг

оқибатларини бартараф этишга, телекоммуникация тармоқлари, ахборот тизимлари ҳамда ресурслари фаолиятининг барқарорлигини ва ишончлилигини тиклашга қаратилган ҳуқуқий, ташкилий, молиявий-иқтисодий, муҳандислик-техник чора-тадбирлар, шунингдек маълумотларни криптографик ва техник жиҳатдан ҳимоя қилиш чора-тадбирлари мажмуи.

Киберҳужум – кибермаконда аппарат, аппарат-дастурий ва дастурий воситалардан фойдаланган ҳолда қасддан амалга ошириладиган, киберхавфсизликка таҳдид соладиган ҳаракат.

Муҳим ахборот инфратузилмаси – муҳим стратегик ва ижтимоий-иқтисодий аҳамиятга эга бўлган автоматлаштирилган бошқарув тизимларининг, ахборот тизимлари ҳамда тармоқлар ва технологик жараёнлар ресурсларининг мажмуи.

Муҳим ахборот инфратузилмаси объектлари – давлат бошқаруви ва давлат хизматлари кўрсатиш, мудофаа, давлат хавфсизлигини, ҳуқуқ-тартиботни таъминлаш, ёқилғи-энергетика мажмуи (атом энергетикаси), кимё, нефть-кимё тармоқлари, металлургия, сувдан фойдаланиш ва сув таъминоти, қишлоқ хўжалиги, соғлиқни сақлаш, уй-жой коммунал хизматлар кўрсатиш, банк-молия тизими, транспорт, ахборот-коммуникация технологиялари, экология ва атроф-муҳитни муҳофаза қилиш, стратегик аҳамиятига эга бўлган фойдали қазилмаларни қазиб олиш ва қайта ишлаш соҳасида, ишлаб чиқариш соҳасида, шунингдек иқтисодиётнинг бошқа тармоқларида ва ижтимоий соҳада қўлланиладиган ахборотлаштириш тизимлари [7].

Муҳим ахборот инфратузилмаси субъектлари – давлат органлари ва ташкилотлари, шунингдек мулк, ижара ҳуқуқлари асосида ёки бошқа қонуний асосларда муҳим ахборот инфратузилмаси объектларига эгалик қилувчи юридик шахслар, шу жумладан муҳим ахборот инфратузилмаси объектларининг ишлашини ҳамда ҳамкорлигини таъминловчи юридик шахслар ва (ёки) якка тартибдаги тадбиркорлар.

Кибертерроризм – террористик мақсадлар йўлида компьютер ва телекоммуникация технологиялари (асосан Интернет)дан фойдаланиш. Кибертерроризм, шунингдек, махсус хакер дастурлари орқали компьютер бошқаруви тармоқларини эгаллаб олиш ва компьютер вируслари ёрдамида Интернет тармоғида теракт содир этиш, Интернет тармоғини ишдан чиқаришни кўзда тутади. Ушбу термин биринчи маротаба 1980 йилларда АҚШдаги Хавфсизлик ва разведка институти (Institute for Security and Intelligence) катта илмий ходими Барри Коллин томонидан ишлатилган.

Киберфирибгарлик – бу Интернет тармоғи орқали бузғунчининг атайин бирор-бир кимсага моддий ёки маънавий етказиши жараёни. Бугунги кунда киберфирибгарликнинг яққол кўриниши – жабрдийданинг молиявий маълумотларини ўғринча қўлга киритган ҳолда, унга моддий ва маънавий зарар етказишда намоён бўлмоқда.

Киберхужум – (Cyber attack) бу шахсий ёки уюшган гуруҳ томонидан компьютер тармоқлари, ахборот тизимлари ёки катта АТ инфратузилмасини нишонга олиш учун зарарли кодни ўғирлаш, ўзгартириш ушбу турдаги ҳаракатларнинг хар қандай афзалликларидан фойдаланиш учун турли хил воситалардан фойдаланган холда ишлатиладиган ҳужум турлари ҳисобланади.

Интернет браузерини бузиш – (Browser Hijacking) бу сизнинг веб браузерингиздан стандарт уй саҳифасини ёки қидирув тизимини рухсатсиз зарарли дастурлар орқали ўзгартириш жараёни. Фойдаланувчи таъсирланган ўзгаришларни қайтариб бўлмаслигини сезиши мумкин ва ушбу турдаги дастур учун ҳимоя воситасидан фойдаланиш керак. Бу тизимнинг умумий хавфсизлигига жиддий таҳдид деб ҳисобламайди, аммо уни тезда йўқ қилиш керак, чунки у Интернетдан фойдаланиш самарадорлигига таъсир қилади.

Компьютердан ноқонуний мақсадларда фойдаланиш – (Computer Abuse) бу компьютердан ахлоқсиз фойдаланиш, масалан фишинг ва зарарли дастурларни тарқатиш, саботаж ҳамда киберҳужумлар.

Хакер – (hacker) одатда хакер деганда зарар етказиш учун компьютер тизимларига рухсатсиз киришни оширадиган шахс тушунилади. Аммо шуни ёдда тутиш лозимки, хакерларнинг икки тури мавжуд: тизимларга бузиб кириш синовларини ўтказиб, хавфсиз тизим ва дастурлар яратишда ёрдам берадиган ҳамда ўз натижаларини ошкор қиладиган “whitehat” хакерлар ҳамда ўз маҳоратларидан фойдаланадиган “blackhat” хакерлар.

Кетфишинг – (catfishing) Интернетда ёки бутун ижтимоий тармоқлардаги гуруҳларда эмоционал/романтик муносабатларда одамларни алдаш мақсадида, сохта профил, аккаунт ёки веб-сайтидан фойдаланган холда мулоқотга киришиб, ўз мақсадларига эришишни ичига олган жараён.

Мутахассислар кетфишинг шахсдаги нафрат, қасос, қизиқувчанлик, ёлғизлик ёки зерикиш натижасида юзага келишини таъкидлайдилар.

Бу каби хатти-ҳаракатлар мамлакатимиз ҳудудида ҳам учраб турибди, бунинг учун Жиноят кодекси 165-моддасига (Товламачилик) кўра жавобгарлик белгиланган.

Буллинг (инг. “дўқ қилиш”, “зўравонлик қилиш”)нинг ижтимоий моҳияти бошқаларни қўрқитиш, камситиш, жисмоний ва руҳий террор қилиш йўли билан ўзига бўйсундириб олиш. Кибербуллинг эса Интернет орқали виртуал тармоқ фойдаланувчиларини, айниқса, ёшларни ҳақоратлаш, камситиш ва шу билан бирга, уларда бундай хатти-ҳаракатларга рағбат уйғотиш жараёнидир.

Грифинг – бу кўпчилик компьютер ўйинчилари иштирокидаги ўйин жараёнида кимнингдир қаттиқ жаҳлини чиқариш, яъни руҳий зарба бериш. Бундай ўйинлар натижасида айрим ҳолларда “жаҳл отига минган” жабрдийда ёшлар ўзига шикаст етказиб қўяди. Грифинг “ўйин ичидаги вандализм” деб ҳам таърифланади. Грифинг билан шуғулланувчи кимсалар “грифёрлар” деб аталади.

Криптолокер – (Cryptolocker) бу 2013 йилда пайдо бўлган Интернет товламачилигининг бир тури бўлиб, унинг мақсади Microsoft Windows ўрнатилган компьютерлардан фойдаланган ҳолда жабрланувчиларни ўзига жалб қилиш кўпгина товламачиларда бўлгани каби, буни тарқатишнинг асосий усули – зарарли қўшимчали электрон почта спамидир. Cryptolocker ҳужумларни бошлаш учун ташқи инфратузилмани ишлатади ва фаоллаштирилганда, маҳаллий қурилмаларда сақланган файллар ва маълумотларни, шунингдек, булутли сақлаш ҳисобларида сақланганларни шифрлайди.

Бу каби хатти-ҳаракатлар мамлакатимиз ҳудудида ҳам учраб турибди, бунинг учун Жиноят кодексининг 165-моддасига (Товламачилик) кўра жавобгарлик белгиланган [8].

Криптовалюта – криптография асосида банкноталарни хавфсиз алмашиш ва узатиш учун марказлаштирилган тизимлар. “Криптовалюта” атамаси 2011 йилда Форбес журналида чоп этилган “Крипто валютаси” Биткоин тизими ҳақидаги мақола эълон қилинганидан кейин ўрнатилди. Шу билан бирга, биткоин яратувчиси ва бошқа кўплаб муаллифлар “электрон пул” атамасини ишлатган. Криптографик усуллар манзилни яратиш ва у билан ишлаш учун ваколатни текшириш механизмларида иштирок этади *(очиқ калитлар тизимига асосланган электрон рақамли имзо, буюртма фақат шу манзилга мос келадиган махфий калит эгасига берилади)*, шунингдек битимлар пакетининг шаклланиши ва унинг бошқа пакетлар билан алоқаси *(бу криптовалютанинг миқдори ҳақидаги маълумотни ўзгартиришни имконсиз қилади)*. Криптовалюта бирликлари маълумотлар бирликларидир. Криптовалютанинг пайдо бўлиши, ўз навбатида, унга тегишли фаолиятнинг пайдо бўлишига олиб келди. Улардан энг кенг тарқалгани майнинг бўлди [9].

Майнинг – бу кўп қиррали ва аниқ таърифланиши қийин бўлган тушунча. Майнинг тармоқдаги битимларни кузатиш ва рақамли имзоларнинг ҳақиқийлигини текшириш, блокчейнни сақлаш ва янги блокларни кузатиш, қўшимчалар учун номзод блокларни яратиш, блокни яроқли ҳолатга келтирадиган криптовалютани топиш *(тўғридан-тўғри қазиб олиш)* ҳамда блокни бошқа иштирокчиларга эълон қилиш каби процедура занжиридан иборат жараён сифатида тавсифланади. Содда қилиб айтганда, майнинг криптовалюта яратишга ва криптовалюта кўринишида мукофот олишга қаратилган фаолият.

Фишинг – (Phishing) бу кибержиноятчилар томонидан фойдаланувчиларнинг конфиденциал маълумотларини тўплаш учун фойдаланадиган Интернет-фирибгарликнинг бир кўриниши. Интернет фирибгарлари жабрланувчиларни ишонишга ва махфий маълумотларни ошкор қилишга мажбурлаш учун ўзларини ишончли юридик шахс сифатида кўрсатадилар. Фишинг орқали тўпланган маълумотлардан молиявий маълумотларни эгаллаш, шахсий маълумотларни ўғирлаш, жабрланувчининг ҳисоб рақамларига ёки улар

кириш ҳуқуқига эга ҳисобларига рухсатсиз, жабрланувчини шантаж қилиш ва бошқалар учун фойдаланиш мумкин[10].

Бу зарарли дастурлардан фойдаланиб содир этилган қилмишлар учун Ўзбекистон Республикаси Жиноят Кодексининг 168-моддаси 2-қисми “в” банди билан, компьютер техникасидан фойдаланган холда фирибгарлик жиноятини содир этганлик ҳамда Жиноят Кодекси 165-моддасига асосан товламачилик учун жавобгарлик белгиланган

Алткоинлар – Биткоиндан бошқа барча рақамли валюталар алткоинлар атамаси билан номланади ва тўғридан-тўғри таржимаси “муқобил тангалар” *(баъзида пастки тангалар деб ҳам юритилади)* маъносини беради [11]. Уларнинг барчаси биткоиндан сўнг яратилган ва тақлид валюталар ҳисобланади. Биткоин ва алткоинлар ўртасида сезиларли ва яширин фарқлар кўп. Мисол учун, Лайткоин *(Litecoin)* ҳар бир блокни 2.5 дақиқада жарёнлаштиради. Солиштириш учун, биткоин блокчейнида бир блок учун кетадиган вақт 10 минутдан ошиқроқ вақт талаб қилади. Бу шуни англатадики, лайткоин билан валюта ўтказмалар анчагина тезроқ амалга оширилади. Яна бир мисол, Ethereumни олайлик. Ethereum ўз тармоғида “ақлли шартномалар” *(smart contracts)* асосида марказлаштирилмаган эркин программаларни тузишга имкон беради. Блумбергнинг хабар беришича, 2020 йилда Ethereum энг оммабоп шифрланган валютага деб топилган.

Биткоин – амалиётларни ҳисобга олиш учун шу номдаги бирликдан фойдаланувчи пиринг тўлов тизими[12]. Биткоинлар криптовалюта, виртуал валюта, рақамли валюта ва электрон нақд пул сифатида таснифланади. Қачонлардир чиқариладиган биткоинларнинг умумий сони 21 миллионни ташкил этади. Биткоинлардан фойдаланиш мумкин бўлган мамлакатларда айрим мол ва хизматларни харид қилиш учун фойдаланиш мумкин. Кўпинча биткоинлардан сармоя асбоби ёки криптовалюта биржаларида оддий валютага айирбошлаш воситаси сифатида фойдаланишади.

Биткоин нархи таклиф ва талаб мувозанатига боғлиқ бўлиб, уни ҳеч ким тартибга солмайди. Шунинг учун биткоинни баъзан “марказсизлаштирилган валюта” деб аташади.

Биткоин тўловлари хавфсизлиги очиқ калитли криптография билан кафолатланади. Уларнинг ҳақиқийлиги тармоққа уланган минглаб компьютерлар томонидан бажариладиган мураккаб математик ҳисоблар орқали тасдиқланади – бу жараён биткоинлар майнинги деб аталади. Тизим манзиллари ўртасидаги барча транзакциялар ҳақидаги маълумотларни очиқ ҳолда олиш мумкин.

Оммавий шифрлаш (Bulk Encryption) – бу Интернетда хавфсизлик бузилиши ва ахборотни эгаллаб олишдан ҳимоя қилишни таъминлаш учун маълумотларни узатиш, шифрлаш ва шифрлашга керакли воситаларни таъминлайдиган хавфсизлик протоколлар тўплами.

Фаолият сифатини яхшилайдиган ушбу ўзгаришлар билан бир қаторда жиноятчиликнинг янги тури ҳисобланган “Ахборот технологиялари жиноятлари” ҳам бир вақтнинг ўзида шаклий жиҳатдан ўзгариб, янгиланиб бормоқда.

Ушбу соҳадаги жиноятларнинг хавфи шундаки, мудофаа, ишлаб чиқариш, иқтисодий, банк ва бошқа мақсадлардаги мураккаб компьютер тизимларининг бошқарув сенсорлари билан боғлиқ ҳаракатлар учун муҳим бўлган маълумотларнинг йўқ қилиниши, блокланиши, модификацияси одамларнинг ўлимига ва уларнинг соғлиғига зарар етказиши, мулкни йўқ қилиши, катта миқёсда иқтисодий зарар етказиши мумкин.

Ахборот технологиялари соҳасидаги жиноятларга Интернет орқали зарарли вирусларнинг тарқалиши, паролларни бузиш, банк карталари рақамлари ва бошқа банк маълумотларини ўғирлаш, фишинг, ноқонуний маълумотларни тарқатиш (туҳмат, порнографик материаллар, этник ва диний адоватни қўзғатадиган материаллар, этник ва диний адоватни қўзғатадиган материаллар ва бошқалар), Шунингдек, турли хил тизимларнинг ишлашига компьютер тармоқлари орқали зарарли оқибатга олиб келадиган даражада аралашиш киради.

Ахборот технологиялари соҳасидаги жиноятлар олдини олиш юзасидан қўйидаги таклифларни илгари суриш мумкин

Ҳуқуқий ва ташкилий таклифлар

Қонунчиликни доимий янгилаш: *кибержиноятларнинг янги турлари (масалан, дийпфейк ёки крипто-фирибгарлик) учун аниқ жавобгарликни белгилаш ва жиноят кодексига тегишли ўзгартиришлар киритиш.*

Халқаро ҳамкорликни кучайтириш: *кибержиноятчилар кўпинча бошқа давлат ҳудудидан туриб ҳужум қилади. шу сабабли, интерпол ва бошқа халқаро ташкилотлар билан тезкор маълумот алмашинувини йўлга қўйиш.*

Махсус кибер-прокуратура ва судлар: *рақамли далиллар билан ишлаш мураккаб бўлгани учун, ушбу соҳада чуқур билимга эга бўлган терговчи ва судьялар корпусини шакллантириш.*

Техник ва инфратузилмавий чоралар

Миллий киберхавфсизлик марказини ривожлантириш: *давлат органлари ва муҳим инфратузилма объектларига бўлаётган ҳужумларни реал вақтда аниқловчи ва тўсувчи ягона тизимни кучайтириш.*

Шубҳали транзакциялар мониторинги: *банклар ва тўлов тизимларида сунъий интеллект ёрдамида фирибгарлик транзакцияларини автоматик равишда тўхтатиб қолиш тизимини такомиллаштириш.*

Таълим ва аҳолининг рақамли саводхонлиги

"Кибер-гигиена" дарслари: *мактаб ва олий-таълимларда интернетда хавфсизлик қоидалари, фишинг ҳаволаларини таниш ва шахсий маълумотларни ҳимоя қилиш бўйича мажбурий курсларни жорий этиш.*

Оммавий тарғибот: *тв ва ижтимоий тармоқлар орқали фирибгарларнинг энг кўп ишлатадиган усуллари (масалан, "пластик картангиз блокланди" каби алдовлар) ҳақида доимий роликлар намойиш этиш.*

Махсус "бот"лар ва иловалар: *фуқароларга шубҳали ҳавола ёки рақамларни текшириб берадиган бепул давлат хизматларини яратиш.*

Хулоса ўрнида шуни таъкидлашимиз зарурки, айнан кибержиноятларнинг 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. Бу эса юқорида таъкидлаб ўтилган муаммолар юзасидан тегишил чоратадбирларни амалга ошириш ва бу борада тўғри сиёсат юритишимиз зарурлигини кўрсатади.

Фойдаланилган адабиётлар

1. Ўзбекистонда Интернетнинг ривожланиш тенденциялари // Электрон манба http://nargis.uz/article_view.php?id=330
2. https://sud.uz/wp-content/uploads/2021/odilsudlov/5_uz.pdf
3. https://kun.uz/news/2022/04/18/kiberxavfsizlik-togrisidagi-qonun-dxxga-qanday-yangi-vakolatlar-berildi
4. Матчанов А.А. О профилактике правонарушений и преступлений в сфере информационно-коммуникационных технологий (киберпреступлений) //Конституциявий ва маъмурий ҳуқуқ фанларининг замонавий муаммолари ва уларнинг ечимлари: Илмий-амалий конференцияси материаллари (20 йил 10 декабрь). – Т.: Ўбекистон Республикаси ИИВ Академияси, 2021. – С. 78-85
5. https://lex.uz/uz/docs/5960604
6. Ахборот технологиялари сохасида, шу жумладан Интернет тармоғида содир этиладиган ҳуқуқбузарлик ҳамда жиноятларни аниқлаш, барвақт олдини олиш ва тергов қилиш методологияси: – Т.: Ўз.Рес.ИИВ Академияси, 2022. – 8-б.
7. Матчанов А.А. Особенности совершенствования предупреждения, раскрытия и расследования киберпреступлений// Мирзо Улуғбек номидаги Ўзбекистон Миллий Университети илмий журнали. ЎзМУ Хабарлари, Вестник НУУз, ACTA NUUz – Тошкент 2022, 1/12 – С.95-98.
8. Матчанов А.А. Методика расследования киберпреступлений: Монография – Т.: Академия МВД Республики Узбекистан, 2015. – 148 с.
9. Матчанов А.А., Хасанов Ш.Ш. Киберхавсизлик ва кибержиноятлар: Ўқув қўлланма. – Т.: Ўзбекистон Республикаси ИИВ Академияси, 2022. – 54 б.
10. Матчанов А.А. Об особенностях получения доказательств в электронной (цифровой) форме при расследовании киберпреступности // Взаимная правовая помощь в получении электронных доказательств и расследовании трансграничных