ЎЗБЕКИСТОН РЕСПУБЛИКАСИ ЖАМОАТ ХАВФСИЗЛИГИ УНИВЕРСИТЕТИ ҲУЗУРИДАГИ ИЛМИЙ ДАРАЖАЛАР БЕРУВЧИ DSc. 32/30.12.2020.Yu/74.01 РАҚАМЛИ ИЛМИЙ КЕНГАШ

ЎЗБЕКИСТОН РЕСПУБЛИКАСИ ЖАМОАТ ХАВФСИЗЛИГИ УНИВЕРСИТЕТИ

АНОРБОЕВ АМИРИДДИН УЛУҒБЕК ЎҒЛИ

КИБЕРЖИНОЯТЛАРНИНГ ЖИНОИЙ-ҲУҚУҚИЙ ЖИҲАТЛАРИ

12.00.08 – Жиноят ҳуқуқи. Криминология. Жиноят-ижроия ҳуқуқи

Юридик фанлар бўйича фалсафа доктори (PhD) диссертацияси АВТОРЕФЕРАТИ

Тошкент – 2021

УДК: 343.140.02:004.9

Докторлик (PhD) диссертацияси автореферати мундарижаси
Оглавление автореферата докторской диссертации (PhD)
Content of the abstract of the doctoral (PhD) dissertation

ЎЗБЕКИСТОН РЕСПУБЛИКАСИ ЖАМОАТ ХАВФСИЗЛИГИ УНИВЕРСИТЕТИ ҲУЗУРИДАГИ ИЛМИЙ ДАРАЖАЛАР БЕРУВЧИ DSc. 32/30.12.2020.Yu/74.01 РАҚАМЛИ ИЛМИЙ КЕНГАШ

ЎЗБЕКИСТОН РЕСПУБЛИКАСИ ЖАМОАТ ХАВФСИЗЛИГИ УНИВЕРСИТЕТИ

АНОРБОЕВ АМИРИДДИН УЛУҒБЕК ЎҒЛИ

КИБЕРЖИНОЯТЛАРНИНГ ЖИНОИЙ-ҲУҚУҚИЙ ЖИҲАТЛАРИ

12.00.08 – Жиноят ҳуқуқи. Криминология. Жиноят-ижроия ҳуқуқи

Юридик фанлар бўйича фалсафа доктори (PhD) диссертацияси АВТОРЕФЕРАТИ

Тошкент – 2021

Фалсафа доктори (PhD) диссертация мавзуси Ўзбекистон Республикаси Вазирлар Маҳкамаси ҳузуридаги Олий аттестация комиссияси B2019.1.PhD/Yu274 рақам билан рўйхатга олинган.

Диссертация Ўзбекистон Республикаси Жамоат хавфсизлиги университетида бажарилган.

Диссертация автореферати уч тилда (ўзбек, рус, инглиз) Ўзбекистон Республикаси Жамоат хавфсизлиги университети веб-сайти (www.mgjxu.uz) ҳамда «Ziyonet» Ахборот таълим порталида (www.ziyonet.uz) жойлаштирилган.

Илмий раҳбар:	**Рустамбаев Мирзаюсуп Хакимович,** юридик фанлар доктори, профессор
Расмий оппонентлар:	**Инагамджанова Зумратхон Фатхуллаевна** юридик фанлар доктори, профессор
	Расулев Абдулазиз Каримович юридик фанлар доктори, профессор
Етакчи ташкилот:	**Ўзбекистон Республикаси Бош прокуратураси Академияси**

Диссертация ҳимояси Ўзбекистон Республикаси Жамоат хавфсизлиги университети ҳузуридаги илмий даражалар берувчи DSc. 32/30.12.2020.Yu/74.01 рақамли илмий кенгашнинг 2021 йил «27» ноябрь куни соат 10-00даги мажлисида бўлиб ўтади (Манзил: 100109, Тошкент вил., Зангиота тумани, Чорсу қўрғони. Тел.: (99871) 230-32-71; факс: (998971) 230-32-50; e-mail: mgjxu@umail.uz).

Диссертация билан Ўзбекистон Республикаси Жамоат хавфсизлиги университети Ахборот-ресурс марказида танишиш мумкин (2166/1 рақами билан рўйхатга олинган). Манзил: 100109, Тошкент вил., Зангиота тумани, Чорсу қўрғони. Тел.: (99871) 230-32-71; факс: (998971) 230-32-50.

Диссертация автореферати 2021 йил 12 ноябрда тарқатилди.

(2021 йил 12 ноябрдаги 9-рақамли реестр баённомаси).

Д.М. Миразов
Илмий даражалар берувчи илмий кенгаш раиси ўринбосари, юридик фанлар доктори, профессор

М.М. Нурматов
Илмий даражалар берувчи илмий кенгаш илмий котиби, юридик фанлар доктори, доцент

М.Б. Усмонов
Илмий даражалар берувчи илмий кенгаш қошидаги илмий семинар раиси, юридик фанлар доктори, профессор.

КИРИШ (докторлик (PhD) диссертацияси аннотацияси)

Диссертация мавзусининг долзарблиги ва зарурати. Дунёда давлатларнинг ахборот тизимлари ва ресурсларига, халқаро ташкилотлар ва компанияларнинг маълумотлар базасига, молия институтларининг ахборот-коммуникация технологияларига ҳамда инсон ҳуқуқ ва манфаатларига путур етказаётган энг хавфли қилмишлардан бири кибержиноятлар ҳисобланади. Хусусан, кибержиноятларни таҳлил қилувчи халқаро Cybersecurity Ventures ташкилоти экспертларининг фикрича, «дунё бўйлаб ҳар 14 сонияда битта киберҳужум содир этилмоқда, унинг натижасида Жаҳон иқтисодий форумининг прогнозига кўра, 2022 йилда 8 триллион доллар миқдорида дунё давлатлари зарар кўриши мумкин»[1]. Шунинг учун ҳам бугунги кунда, ушбу хавфнинг олдини олиш, унга қарши курашиш ва унинг келиб чиқиш сабабларини бартараф қилиш учун кибержиноятларга қарши курашишнинг самарали механизмларини ишлаб чиқиш ҳамда киберхавфсизликни таъминлашнинг комплекс асосларини яратиш жиноят ҳуқуқи соҳаси учун муҳим аҳамият касб этмоқда.

Жаҳонда кибержиноятларнинг бошқа жиноятларга қараганда янада кенг қамровли хусусиятга эга эканлиги, уларнинг бир мамлакат ҳудудидан туриб, иккинчи мамлакат ҳудудида ҳам содир этилиши мумкинлиги, трансчегаравий жиноят ҳисобланиши, кибержиноятчилар учун иқтисодий томондан уни амалга ошириш самарали ва вақт нуқтаи назаридан тезкор аҳамиятга эга эканлиги, бир лаҳзада жуда кўп миқдорда моддий-маънавий зарарни келтириб чиқариши мумкинлиги ва ушбу соҳада ташкилий-ҳуқуқий механизмлар борасида тизимли муаммоларнинг мавжудлиги инобатга олиниб, киберхавфсизликни таъминлаш бўйича илмий тадқиқот ишлари амалга оширилмоқда. Ҳозирги кунда барча дунё давлатлари учун миллий ва халқаро жиноий-ҳуқуқий муносабатларда кибержиноятларга нисбатан жавобгарликни белгиловчи норматив-ҳуқуқий ҳужжатларни қайта кўриб чиқиш, киберхавфсизликка оид халқаро нормаларнинг миллий қонунчилик билан ўзаро уйғунлаштириш, давлатларнинг кибержиноятларга оид жиноят қонунчилигини ўзаро бирхиллаштириш орқали ушбу жиноятларга қарши ялпи курашиш мехнизмини яратиш ва киберхавфсизликни таъминлаш бўйича халқаро ҳамкорлик ва шерикчилик алоқаларини йўлга қўйиш ва киберхавфсизликни таъминлашнинг самарали илмий-назарий ва амалий ечимини топиш ҳамда илмий таҳлил қилиш устувор вазифа ҳисобланмоқда.

Республикамизда қонун устуворлигини таъминлаш ва суд-ҳуқуқ тизимини янада ислоҳ қилишнинг устувор йўналишларида кенг қамровли дастурий тадбирлар изчил амалга оширилмоқда. 2017–2021 йилларда Ўзбекистон Республикасини ривожлантиришнинг бешта устувор йўналиши бўйича Ҳаракатлар стратегиясида «жиноят ва жиноят-процессуал қонунчилигини такомиллаштириш ва либераллаштириш, алоҳида жиноий қилмишларни декриминаллаштириш, жиноий жазолар ва уларни ижро этиш

[1] https://www.tadviser.ru.

тартибини инсонпарварлаштириш; жиноятчиликка қарши курашиш ва ҳуқуқбузарликларнинг олдини олиш борасидаги фаолиятни мувофиқлаштиришнинг самарадорлигини ошириш; диний экстремизм ва терроризмга, уюшган жиноятчиликнинг бошқа шаклларига қарши курашиш бўйича ташкилий-амалий чораларни кучайтириш» каби муҳим вазифалар белгиланган[1]. Бу эса, кибержиноятларнинг келиб чиқиш сабаблари ва омилларини ўрганиш, кибержиноятларни юридик таҳлил қилиш ва бу каби ижтимоий хавфли қилмишларнинг олдини олиш бўйича зарур илмий тадқиқот ўтказиш зарурлигидан далолат беради.

Ўзбекистон Республикаси Президентининг 2017 йил 7 февралдаги «Ўзбекистон Республикасини янада ривожлантириш бўйича Ҳаракатлар стратегияси тўғрисида»ги ПФ–4947-сон, 2018 йил 13 июлдаги «Суд-ҳуқуқ тизимини янада такомиллаштириш ва суд ҳокимияти органларига ишончни ошириш чора-тадбирлари тўғрисида»ги ПФ–5482-сон Фармон ҳамда 2018 йил 14 майдаги «Жиноят ва жиноят-процессуал қонунчилиги тизимини тубдан такомиллаштириш чора-тадбирлари тўғрисида»ги ПҚ–3723-сон ва 2020 йил 3 сентябрдаги «Суд ҳокимияти органлари фаолиятини рақамлаштириш чора-тадбирлари тўғрисида»ги ПҚ–4818-сон қарорлари, Вазирлар Маҳкамасининг «Давлат ва хўжалик бошқаруви органларининг виртуал маконда иштирокини фаоллаштириш концепциясини тасдиқлаш тўғрисида» 2018 йил 7 августдаги 622-сон қарори ва соҳага оид бошқа қонунчилик ҳужжатларида назарда тутилган вазифалар ижросини амалга оширишда муайян даражада хизмат қилади.

Тадқиқотнинг республика фан ва технологиялари ривожланишининг устувор йўналишларига мослиги. Тадқиқот илм-фанни ривожлантиришнинг «III. Юқори малакали илмий ва муҳандис кадрлар тайёрлаш ҳамда уларни илмий фаолиятга йўналтириш» устувор йўналишига мувофиқ бажарилган.

Муаммонинг ўрганилганлик даражаси. Ўзбекистон Республикасида кибержиноятларга қарши курашиш ва киберхавфсизликни таъминлашга оид масалалар комплекс шаклда етарли даражада ўрганилмаган, фақатгина унинг айрим жиҳатлари ўрганилганлигини таъкидлаш лозим. Чунончи, И.Р.Бегишев киберфирибгарлик жиноятларини, Ҳ.Р.Очилов ўзгалар мулкини компьютер воситаларидан фойдаланиб талон-торож қилганлик учун жавобгарлик чораларини, Ш.Ғойибназаров, И.И.Аминов, М.М.Мирхаётов кибертерроризм ва кибертерроризмни молиялаштириш жиноятларини, А.А.Исманова киберэкстремизм жиноятларини, И.М.Норбўтаев жамоат тартибига қарши қаратилган жиноятларни, Н.Ражабова ахборот-коммуникация технологиялари орқали ўзини ўзи ўлдириш даражасига етказиш ва (ёки) ўзини ўзи ўлдиришга ундаш жиноятларини, А.К.Расулев ахборот технологиялари ва хавфсизлиги соҳасидаги жиноятларга қарши

[1] Ўзбекистон Республикаси Президентининг «Ўзбекистон Республикасини янада ривожлантириш бўйича Ҳаракатлар стратегияси тўғрисида» 2017 йил 7 февралдаги ПФ–4947-сон Фармони // lex.uz – Ўзбекистон Республикаси қонунчилик маълумотлари миллий базаси.

курашишнинг жиноят-ҳуқуқий ва криминологик чораларини такомиллаштириш йўлларини, У.Ф.Хасанов компьютер ахборотидан қонунга хилоф равишда (рухсатсиз) фойдаланиш жиноятларини, А.Хаджаев, Н.Юсупова компютер жиноятларига қарши курашиш йўлларини, Д.Р.Иргашев, М.А.Рахматуллаев блокчейннинг маълумотлар хавфсизлигини ошириши ҳолатини тадқиқ этганлар. Шунингдек, рус олимларидан К.Н.Евдокимов Россия компьютер жиноятчилигини, Т.Л.Тропина компьютер саботажи жиноятларини, Р.И.Дремлюга Интернет орқали содир этиладиган жиноятларни, В.В.Хилюта киберталончилик жиноятларини, Е.В.Тищенко компьютер жинояти ёки Интернет жиноятчилиги учун жиноий жавобгарлик хусусиятларини, В.О.Голубэв трансмиллий компьютер жиноятчилигига қарши курашиш муаммоларини, С.И.Ушаков компьютер ахбороти соҳасидаги жиноятларнинг амалий ва назарий қоидаларини, Е.Щербак ва Н.Щербак компьютер жиноятчилигини квалификация қилиш хусусиятларини, А.А.Данельян хавфсиз кибермаконни яратишнинг халқаро ҳуқуқий жиҳатларини ўрганишган[1].

Кибержиноятчиликка қарши курашиш ва киберхавфсизликни таъминлаш соҳасида комплекс тадқиқотлар М. Маклюэн (Канада), Т.Стоуньер (Буюк Британия), Й. Масуда (Япония), R.Haeni, F.Schreier, B.Weekes, T.H.Winkler (Германия) ва бошқалар томонидан амалга оширилган. Шунингек, Nationales Cyber-Abwehrzentrum-NCAZ (Германия), Australian Cyber Security Center-ACSC (Австралия), National Cyber Security Centre (Ирландия), National Cybersecurity Center-NCSC (Буюк Британия), Национальный координационный центр по компьютерным инцидентам-НКЦКИ (Россия), National Cybersecurity Center-NCSC (АҚШ) марказларида, Ўзбекистонда эса, Ўзбекистон Республикаси Президентининг 2019 йил 14 сентябрдаги «Ахборот технологиялари ва коммуникацияларининг жорий этилишини назорат қилиш, уларни ҳимоя қилиш тизимини такомиллаштиришга оид қўшимча чора-тадбирлар тўғрисида»ги ПҚ–4452-сон қарори билан ташкил қилинган «Киберхавфсизлик маркази» давлат унитар корхонаси томонидан ҳам киберхавфсизлик масалалари ўрганилади.

Диссертация мавзусининг диссертация бажарилаётган олий таълим муассасасининг илмий-тадқиқот ишлари режалари билан боғлиқлиги. Диссертация мавзуси «Ўзбекистон Республикаси Миллий гвардияси Ҳарбий-техник институтида жиноятчилик ва ҳуқуқбузарликнинг содир этилишига имкон бераётган сабаб ва шарт-шароитларни бартараф этиш бўйича режаси» доирасида амалга оширилган.

Тадқиқотнинг мақсади кибержиноятларнинг жиноий-ҳуқуқий жиҳатларини таҳлил қилиш, киберхавфсизликни таъминлаш бўйича илмий-амалий таклиф ва тавсиялар ишлаб чиқишдан иборат.

[1] Мазкур олимлар асарларининг тўлиқ рўйхати диссертациянинг фойдаланилган адабиётлар рўйхатида берилган.

Тадқиқотнинг вазифалари:

кибержиноят тушунчаси ва унинг моҳиятини очиб бериш;

жиноят қонунчилигида кибержиноятлар учун жавобгарликни тизимлаштириш заруриятини ўрганиш;

кибержиноятларни таснифлаш орқали уларни таҳлил қилиш;

шахснинг ҳаёти, соғлиғи, ахлоқи, ҳуқуқ ва манфаатларига қарши қаратилган кибержиноятларни юридик таҳлил қилиш;

ижтимоий-сиёсий кибержиноятларни таҳлил қилиш;

иқтисодиёт соҳасидаги кибержиноятларни таҳлил қилиш;

ахборот-коммуникация технологияларига қарши қаратилган кибержиноятларнинг юридик таҳлилини очиб бериш;

кибержиноятлар учун жазо тайинлашнинг ўзига хос хусусиятларини таҳлил қилиш;

кибержиноятлар профилактикасини такомиллаштириш истиқболларини белгилаш ва қонунчиликни такомиллаштиришга қаратилган таклиф ва тавсиялар ишлаб чиқишдан иборат.

Тадқиқотнинг объектини Ўзбекистон Республикасида кибержиноятларнинг жиноий-ҳуқуқий жиҳатларини ҳуқуқий тартибга солиш билан боғлиқ бўлган ижтимоий муносабатлар ташкил қилади.

Тадқиқотнинг предметини кибержиноятларнинг назарий-ҳуқуқий таҳлили, кибержиноятларнинг юридик таҳлили, кибержиноятлар учун жазо тайинлаш ва кибержиноятлар профилактикасини такомиллаштириш истиқболлари билан боғлиқ масалалар ташкил этади.

Тадқиқотнинг усуллари. Тадқиқот давомида анализ, синтез, дедукция, индукция, қиёсий-ҳуқуқий таҳлил, тарихийлик, анкета сўрови, эмпирик материаллар ва статистик маълумотлар таҳлили, кузатув, тизимли ёндошув, мантиқийлик каби тадқиқот усуллари қўлланилган.

Тадқиқотнинг илмий янгилиги қуйидагилардан иборат:

давлат идоралари ва ташкилотларнинг дастурий таъминотлари, маълумотлар базалари, шу жумладан операцион тизимларининг ахборот ва киберхавфсизлик талабларига мувофиқлиги юзасидан уларни мажбурий экспертизадан ўтказиш механизмини жорий этиш асослаб берилган;

веб-сайт фойдаланувчилари томонидан қолдирилган шарҳлар матнида, шунингдек ижтимоий тармоқлар ёки мессенжерларда Ўзбекистон Республикаси Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлиги томонидан чекланадиган маълумотлар аниқланса, Ўзбекистон Республикаси Президенти Администрацияси ҳузуридаги Ахборот ва оммавий коммуникациялар агентлигининг Оммавий коммуникациялар масалалари бўйича маркази томонидан веб-сайт, веб-сайт ва (ёки) мессенжер саҳифаси эгаси, шунингдек блогерга Ўзбекистон Республикаси қонунчилиги билан тарқатилиши тақиқланган ахборотларни олиб ташлаш тўғрисида хабарнома юборилиши асослантирилган;

карантинли ва инсон учун хавфли бўлган бошқа юқумли касалликларнинг пайдо бўлиши ҳамда тарқалиши шароитида карантинли ва инсон учун хавфли бўлган бошқа юқумли касалликлар тарқалиши ҳақида

ҳақиқатга тўғри келмайдиган маълумотларни нашр қилиш ёки бошқача усулда кўпайтирилган матнда ёки оммавий ахборот воситалари, шунингдек Интернет тармоғи орқали тарқатиш учун жиноий жавобгарликни белгилаш асослаб берилган;

порнографик, зўравонликни ёки шафқатсизликни тарғиб қилувчи маҳсулотни тарқатиш, реклама қилиш, намойиш этиш мақсадида тайёрлаш ёки Ўзбекистон Республикаси ҳудудига олиб кириш, худди шунингдек порнографик маҳсулотни реклама қилиш, намойиш этиш, тарқатиш, шу жумладан оммавий ахборот воситаларида, телекоммуникация тармоқларида ёки Интернет жаҳон ахборот тармоғида реклама қилиш, намойиш этиш, тарқатиш учун жиноий жавобгарликни белгилаш асосланган.

Тадқиқотнинг амалий натижалари қуйидагилардан иборат:

киберхавфсизликни тартибга солиш соҳасида ваколатли орган сифатида Давлат хавфсизлик хизматини белгилаш ҳақидаги таклифлар ягона технологик ёндашув асосида давлат ва хўжалик бошқаруви органлари, маҳаллий давлат ҳокимияти органлари, бошқа ташкилотлар ва идораларда ахборот-коммуникация технологияларини жорий этиш ва ривожлантириш ҳамда ахборот хавфсизлиги ҳолатини назорат қилиш, мониторинг қилиш, ўрганиш ва текширишни амалга оширишга хизмат қилади;

олий таълим муассасаларида киберхавфсизлик соҳаси бўйича бакалавриат босқичида таълим йўналишини очиш ҳамда кадрлар тайёрлаш тизимини йўлга қўйиш ҳақидаги таклифлар ахборот технологиялари ва киберхавфсизлик йўналишларида юқори малакали мутахассисларнинг тайёрланишига хизмат қилади;

ахборот-коммуникация технологиялари соҳасига оид таклифлар рақамли иқтисодиёт ва электрон ҳукуматни ривожлантириш доирасида ахборот тизимлари, ресурслари ва бошқа дастурий маҳсулотларни яратиш ва жорий этиш бўйича давлат органлари ва ташкилотларнинг лойиҳалари ҳамда норматив-ҳуқуқий ҳужжатлари лойиҳалари Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигида мажбурий экспертизадан ўтказиш ваколатлари белгиланишига ҳамда электрон ҳукумат ва рақамли иқтисодиёт лойиҳаларини амалга оширишда ягона технологик ёндашувни таъминлаш, шу жумладан лойиҳавий-техник ҳужжатларни комплекс экспертизадан ўтказиш «Электрон ҳукумат лойиҳаларини бошқариш маркази» давлат муассасасининг асосий вазифа ва функцияларидан бири бўлишига хизмат қилади;

ахборот хавфсизлиги соҳасида кадрларни ахборот хавфсизлиги, киберхавфсизлик ва жамоат хавфсизлиги соҳасида ўқитиш тизимини такомиллаштириш, ахборот ва киберхавфсизлик соҳасида халқаро ҳамкорликни ташкил этиш, жамоат тартибини таъминлаш ва шахсий маълумотларни ҳимоя қилиш, халқаро ташкилотлар ва хорижий мамлакатлар билан ўзаро фойдали ҳамкорликни кенгайтириш, давлат ва хўжалик бошқаруви органлари, маҳаллий ижро этувчи ҳокимият органларининг ахборот ресурслари ва тизимлари киберхавфсизлигини таъминлаш соҳасида давлат сиёсати амалга оширилишини ташкил этиш, шунингдек, миллий

ахборот маконининг яхлитлигини сақлаш чора-тадбирларини кўриш бўйича Вазирлар Маҳкамасининг ваколатларини белгилаш ҳақидаги таклифлар Вазирлар Маҳкамасининг IT-технологиялар, телекоммуникациялар ва инновацион фаолиятни ривожлантириш масалалари департаментининг асосий вазифаларини тўлақонли амалга оширишни таъминлашга хизмат қилади;

ўрта муддатга мўлжалланган киберхавфсизликка доир миллий стратегияни ва Ўзбекистон Республикасининг «Киберхавфсизлик тўғрисида»ги Қонуни лойиҳасини ишлаб чиқиш ва қабул қилиш ҳақидаги таклиф ушбу соҳадаги муносабатларнинг ягона қонун ҳужжати билан тартибга солиб қўйилишига хизмат қилади.

Тадқиқот натижаларининг ишончлилиги. Тадқиқот натижаларининг ишончлилиги ишда қўлланилган усуллар, унинг доирасида фойдаланилган назарий ёндашувлар расмий манбалардан олингани, хорижий тажриба ва миллий қонунчилик ҳужжатларининг ўзаро таҳлил қилингани, хулоса, таклиф ва тавсияларнинг амалиётга жорий этилгани, олинган натижаларнинг ваколатли тузилмалар томонидан тасдиқлангани билан изоҳланади. Шу билан бирга, тадқиқот давомида 485 та давлат органи ва идораси, таълим муассасаларига сўровлар юборилди, сўровлар натижалари бўйича кибержиноятлар ва киберхавфсизлик бўйича 485 та ташкилотдан 438 та ташкилот ходимлари зарур даражада тушунчага эга эмаслиги, ташкилотда киберхавфсизликни таъминлаш бўйича лозим даражада кўникма ҳамда моддий-техник таъминот мавжудмаслиги таъкидлашганлиги аниқланди, қолган ташкилотлардан олинган материаллар асосида диссертация мазмун-моҳияти бойитилди.

Тадқиқот натижаларининг илмий ва амалий аҳамияти. Диссертация ишининг илмий аҳамияти шундаки, изланишлар натижасида билдирилган хулоса, таклиф ва тавсиялар жиноят ҳуқуқининг назарий билимларини бойитади ва янги илмий тадқиқотлар олиб боришга имкон яратади ҳамда ундаги илмий-назарий ғоя ва хулосалар Ўзбекистон Республикаси жиноят қонунчилигининг иқтисодий-ҳуқуқий механизмини такомиллаштириш билан боғлиқ масалаларни янада чуқурроқ ўрганишда илмий аҳамият касб этади.

Тадқиқотнинг амалий аҳамияти эса, мавзуни тадқиқ этиш натижасида шакллантирилган илмий қоидалар, хулосалар ва тавсиялардан Ўзбекистон Республикасининг «Кибержиноятларга қарши курашиш тўғрисида», «Киберхавфсизлик тўғрисида», «Киберагрессия тўғрисида»ги қонунлари лойиҳаларини ишлаб чиқишда ҳамда Ўзбекистон Республикаси Жиноят кодексини такомиллаштиришга хизмат қилади. Тадқиқот материлларидан олий юридик таълим муассасаларида «Жиноят ҳуқуқи», «Жиноят процесси», «Криминалистика», «Рақамли криминалистика», «Фуқаролик ҳуқуқи», «Кибернетика», «Информатика», «Ахборот ҳуқуқи» фанлари ўқув жараёнида маъруза ва семинарлар ўтказишда фойдаланиш мумкин.

Тадқиқот натижаларининг жорий қилиниши. Кибержиноятларнинг жиноий-ҳуқуқий жиҳатларини бўйича олиб борилган тадқиқот натижалари асосида:

Республикамиздаги барча давлат органлари ва ташкилотларининг ахборот тизимларининг ахборот ва киберхавфсизлик талабларига мувофиқлиги юзасидан мажбурий экспертизаси тизимини жорий этиш ҳақидаги таклиф Ўзбекистон Республикаси Президентининг 2020 йил 5 октябрдаги ПФ–6079-сон Фармони билан тасдиқланган 2020-2022 йилларда «Рақамли Ўзбекистон – 2030» стратегиясини амалга ошириш бўйича «Йўл харитаси»нинг 28-бандида ўз ифодасини топган *(Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 16.07.2020 йилдаги 32-8/4040-сон, 18.02.2021 йилдаги 32-8/1190-сон ва 26.02.2021 йилдаги 32-8/1451-сон далолатномаси).* Ушбу таклифнинг жорий қилиниши давлат идоралари ва ташкилотларининг ахборот тизимларининг мажбурий экспертизадан ўтказилиши орқали уларнинг киберхавфсизлигини таъминлашга хизмат қилган;

веб-сайт, веб-сайт ва (ёки) мессенжер саҳифаси эгаси, шунингдек блогерга Ўзбекистон Республикаси қонунчилиги билан тарқатилиши тақиқланган ахборотни олиб ташлаш тўғрисида хабарнома юбориш тартибини белгилаш зарурлиги ҳақидаги таклиф Вазирлар Маҳкамасининг «Вазирлар Маҳкамасининг «Бутунжаҳон Интернет тармоғида ахборот хавфсизлигини янада такомиллаштириш чора-тадбирлари тўғрисида» 2018 йил 5 сентябрдаги 707-сон қарорига қўшимчалар киритиш тўғрисида» 2020 йил 23 декабрдаги 807-сон қарорининг 2-банди ва иловасида ўз ифодасини топган. *(Вазирлар Маҳкамасининг 18.02.2021 йилдаги 12/21-04-сон ҳамда Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 18.02.2021 йилдаги 32-8/1190-сон ва 26.02.2021 йилдаги 32-8/1451-сон далолатномаси)*. Ушбу таклифнинг жорий қилиниши бутунжаҳон интернет тармоғига жойлаштирилаётган ноқонуний маълумотларнинг ўз вақтида уни тармоққа жойлаштирган шахс томонидан олиб ташланиши зарурлигига оид муносабатларнинг лозим даражада тартибга солиб қўйилишига хизмат қилган.

Пандемия шароитида аҳоли ўртасида турли хил вахима ва ҳақиқатга тўғри келмайдиган ахборотларнинг чекланишини таъминлаш мақсадида карантинли ва инсон учун хавфли бўлган бошқа юқумли касалликлар тарқалиши ҳақида ҳақиқатга тўғри келмайдиган маълумотларни тарқатиш бўйича жиноий жавобгарликни белгилаш ҳақидаги таклиф Ўзбекистон Республикаси Жиноят кодексининг 244^5-моддасида ўз ифодасини топган *(Ўзбекистон Республикаси Олий Мажлисининг Қонунчилик палатаси Коррупцияга қарши курашиш ва суд-ҳуқуқ масалалари қўмитасининг 22.04.2021 йилдаги 06/1-05/1087-сон ҳамда Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 16.07.2020 йилдаги 32-8/4040-сон, 18.02.2021 йилдаги 32-8/1190-сон ва 26.02.2021 йилдаги 32-8/1451-сон далолатномаси).* Ушбу таклифнинг жорий қилиниши пандемия шароитида карантин ҳақидаги маълумотларга ноқонуний ишлов берилишининг олдини олишга хизмат қилган;

порнографик ва зўравонликни ёки шафқатсизликни тарғиб қилувчи маҳсулотни маҳсулотни телекоммуникация тармоқларида ёки Интернет

тармоғида реклама қилиш, намойиш этиш, тарқатиш учун жавобгарликни белгилаш ҳақидаги таклифлар Ўзбекистон Республикаси Жиноят кодексининг 130 ва 130[1]-моддаларида ўз ифодасини топган *(Ўзбекистон Республикаси Олий Мажлисининг Қонунчилик палатаси Коррупцияга қарши курашиш ва суд-ҳуқуқ масалалари қўмитасининг 22.04.2021 йилдаги 06/1-05/1087-сон ҳамда Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 16.07.2020 йилдаги 32-8/4040-сон, 18.02.2021 йилдаги 32-8/1190-сон ва 26.02.2021 йилдаги 32-8/1451-сон далолатномаси).* Ушбу таклифнинг жорий қилиниши порнографик ва зўравонлик тусидаги маҳсулотларнинг тарқатилиши ва ноқонуний фойдаланилишининг олдини олишга хизмат қилган.

Тадқиқот натижаларининг апробацияси. Тадқиқот натижалари 11 та илмий-амалий анжуманда, хусусан, 5 та халқаро ва 6 та республика илмий-амалий анжуманларида муҳокамадан ўтказилган.

Тадқиқот натижаларининг эълон қилинганлиги. Тадқиқот мавзуси бўйича 22 илмий иш, шу жумладан 1 та монография, 21 та илмий мақола (5 таси хорижий нашрларда) чоп этилган.

Диссертациянинг тузилиши ва ҳажми. Диссертация таркиби кириш, учта боб, хулоса, фойдаланилган адабиѐтлар рўйхати ва иловалардан иборат. Диссертациянинг ҳажми 156 бетни ташкил этади.

ДИССЕРТАЦИЯНИНГ АСОСИЙ МАЗМУНИ

Диссертациянинг кириш (диссертация аннотацияси) қисмида диссертация мавзусининг долзарблиги асосланган, тадқиқотнинг мақсад ва вазифалари ҳамда объект ва предмети тавсифланган, Ўзбекистон Республикаси фан ва технологияси тараққиётининг устувор йўналишларига мослиги кўрсатилган, тадқиқотнинг илмий янгилиги ва амалий натижалари баён қилинган, олинган натижаларнинг назарий ва амалий аҳамияти очиб берилган, тадқиқот натижаларини амалиётга жорий этиш, нашр этилган ишлар ва диссертация тузилиши бўйича маълумотлар келтирилган.

Тадқиқотнинг биринчи боби ***«Кибержиноятларнинг назарий-ҳуқуқий таҳлили»*** деб номланиб, ушбу бобдаги учта параграфда кибержиноят тушунчаси ва унинг моҳияти, жиноят қонунчилигида кибержиноятлар учун жавобгарликни тизимлаштириш зарурияти ва кибержиноятларни таснифлаш билан боғлиқ масалалар таҳлил қилинган.

Ушбу бобнинг *«Кибержиноят тушунчаси ва унинг моҳияти»* деб номланган биринчи параграфи кибержиноят тушунчаси ва унинг доктринал ҳамда расмий тушунчаларининг мазмун-моҳиятини очиб беришга бағишланган.

Диссертант томонидан кибержиноятлар тушунчасига таъриф бериш бевосита ахборот-коммуникация технологияларининг ривожи билан боғлиқ экани ёритилган бўлиб, ушбу тушунча технологиянинг ривожига қараб, «глобал тармоқ жиноятчилиги», «компьютер жиноятчилиги», «компьютер билан боғлиқ жиноят», «компьютер орқали жиноят содир этиш», «электрон

жиноятчилик» ва «юқори технологиялар жиноятчилиги», «виртуал жиноятчилик» каби турлича номланганлиги қайд этилган. Шунингдек, ушбу жиноятларнинг барчаси кибермуҳитда содир этилиши, ушбу қоидани халқаро ҳужжат бўлган Европа Кенгашининг «Компьютер жиноятлари тўғрисида» 2001 йилдаги Конвенцияси қоидаларида ҳам мавжудлиги таъкидланган.

«*Жиноят қонунчилигида кибержиноятлар учун жавобгарликни тизимлаштириш зарурияти*» деб номланган биринчи бобнинг иккинчи параграфида жиноят қонунчилигида кибержиноятлар учун жавобгарликни тизимлаштириш зарурияти асосланган.

Халқаро полиция ассоциациясининг Россия бўлими раҳбари, генерал-лейтенант Юрий Жданов ҳисоб-китобларига кўра, жаҳонда 2019 йилга қараганда 2020 йилда кибержиноятлар сони 71,4 фоизга ошган. Бу борада давлатлар томонидан олиб борилаётган ислоҳотлар натижасида ҳозирги кунда ахборотни муҳофаза қилиш, ахборотни ошкор қилганлик, компьютер жиноятчилиги юзасидан 500 дан зиёд қонунчилик ҳужжатлари мавжудлиги, Ўзбекистонда эса, буни тартибга соладиган алоҳида қонунчилик ҳужжатлари лозим даражада ишлаб чиқилмаганлиги ва қуйидаги ҳолатларни инобатга олиб, мамлакатимизда хавфсиз кибермаконни яратиш борасидаги муносабатларни лозим даражада белгилаб қўйиш зарурияти таъкидланган.

Хусусан, Ўзбекистон Республикаси Президентининг 2017 йил 7 февралдаги ПФ–4947-сон Фармони билан тасдиқланган 2017-2021 йилларда Ўзбекистон Республикасини ривожлантиришнинг бешта устувор йўналиши бўйича Ҳаракатлар стратегиясини «Халқ билан мулоқот ва инсон манфаатлари йили»да амалга оширишга оид давлат дастурининг 297-бандида илк бора расмий норматив-ҳуқуқий ҳужжатда киберхавфсизлик тушунчаси қўлланилиб, бу борада бир қатор ижобий ишлар амалга оширилмоқда. Бироқ, соҳага оид қонунчилик ҳужжатларининг лозим даражада ишлаб чиқилмаганлиги, Жиноят кодексининг 167-169, 278^1-278^7-моддаларида назарда тутилган жиноятнинг воситаси ёки предмети бўлган компьютер тизимлари ёки компьютер техникаси тушунчаси бугунги кунда ўзининг техник имкониятлари туфайли тўлиқ кибержиноятларни қамраб ололмаслиги, хусусан, мобил илова орқали амалга оширилган фирибгарлик жиноятларида мобил илова ўзининг техник имкониятидан келиб чиқиб, компьютер тизими ёки тармоғига кирмаслиги сабабли жиноят қонунчилигимизни қайта кўриб чиқиш зарурлиги асосланган.

«*Кибержиноятларнинг таснифланиши*» деб номланувчи ушбу бобнинг учинчи параграфида кибержиноятларнинг сони жуда кўп бўлганлиги сабабли уларни таснифлаш ва маълум бир гуруҳларга ажратиб ўрганиш таклиф қилинган. Мазкур таклиф ўринли таклиф эканлигини кўрсатиш учун Tadviser, IT Skills, Касперский компаниялари, Бирлашган Миллатлар Ташкилотининг гиёҳванд моддалар ва жиноятчилик бўйича бошқармаси ва Серия модул университети, Жиноий фаолиятдан олинган даромадларни легаллаштиришга ва терроризмни молиялаштиришга қарши кураш бўйича Евросиё гуруҳи олимлари ҳамда олимлар Э.Л.Кочкинанинг, П.С.Титова,

Наре Смбатян, Н.Лимож, М.Косович, Д.В.Пашнев, Э.С.Шевченко, Ю.Газизова, Т.Л.Тропинанинг фикрлари таҳлил қилинган. Филиппинда 2012 йилда қабул қилинган «Кибер жиноятларнинг олдини олиш тўғрисида»ги 10175-сон Филиппин Республикаси қонуни (РА10175) ва у асосида қайта кўриб чиқилган Филиппин Жиноят кодексига асосан истаган қилмиш агарда ахборот-коммуникация технологиялари орқали амалга оширилган бўлса, бу кибержиноят деб ҳисобланади ҳамда мазкур жиноятларни содир этган шахсларга Филиппин Жиноят кодексида назарда тутилган санкциялардаги жазо миқдоридан бир даражага кўп бўлган жазо қўлланилади[1], деган кибержиноятларни таснифлашга оид нормалари ўрганилиб, «Компьютер жиноятлари тўғрисида»ги Будапешт Конвенцияси тадқиқ этилиб, кибержиноятларни қуйидаги гуруҳларга ажратиб ўрганишни таклиф қилинган:

Хусусан, кибержиноятлар амалга ошириш усулига кўра, иккита катта гуруҳга бўлинади, яъни кибертехнологиялардан фойдаланиб содир этиладиган кибержиноятлар ва кибертехнологияларга қарши қаратилган кибержиноятлар. Буни аниқроқ тушунтирадиган бўлсак, кибержиноятлар ахборот-коммуникация технологияларидан фойдаланиб содир этиладиган кибержиноятларга ва ахборот-коммуникация технологияларига нисбатан содир этиладиган жиноятларга бўлинади. Жиноят кодексининг 103-моддасининг иккинчи қисми «г»-банди, 103^1-моддасининг иккинчи қисми «в»-банди, 167-моддасининг учинчи қисми «г»-банди, 168-моддасининг 2-қисми «в»-банди, 169-моддасининг учинчи қисми «б»-банди, 188^1-, 244^1-, 244^5-, 278-моддаларида назарда тутилган ижтимоий хавфли қилмишлар ахборот-коммуникация технологияларидан фойдаланиб, Жиноят кодексининг 278^1-278^7-моддаларида назарда тутилган ижтимоий хавфли қилмишлар ахборот-коммуникация технологияларига нисбатан содир этилган кибержиноятлар саналади.

Кибержиноятларни ижтимоий хавфли қилмишни қайси маконда содир этилишига қараб иккита гуруҳга ажратиш мумкин, яъни ахборот-коммуникация технологиялари соҳасига тегишли кибермаконда содир этиладиган кибержиноятлар ва ахборот соҳасида содир этиладиган кибержиноятлар. Иккала жиноят ҳам кибермуҳитда содир этилади, бироқ ахборот-коммуникация технологиялари соҳасидаги кибержиноятларда ахборот-коммуникация технологияси зарар кўриши ёки зарар етадиган ҳолатга олиб келиниши мумкин. Ахборот соҳасидаги кибержиноятларда эса, ахборот-коммуникация технологияларига зарар етмайди, балки фойдаланувчиларга зарар етказувчи маълумотлар уларнинг ахборот-коммуникация технологиясида сақланиши, узатилиши ва фойдаланиши орқали шахс, жамият ва давлат манфаатларига путур етказилади.

---

[1] Акт, определяющий киберпреступность, обеспечивающий предупреждение, расследование, преследование и назначение наказаний за это и другие цели. Республиканский закон № 10175. 12 сентября 2012 г. https://www.officialgazette.gov.ph/2012/09/12/republic-act-no-10175/.

Кибержиноятлар объектига нисбатан содир этилишига қараб, шахснинг ҳаёти, соғлиғи, ахлоқи, ҳуқуқ ва манфаатларига қарши қаратилган, ижтимоий-сиёсий, иқтисодиёт соҳасидаги, ахборот-коммуникация технологияларига қарши қаратилган кибержиноятларга бўлинади.

Тадқиқотнинг иккинчи боби **«*Кибержиноятларнинг юридик таҳлили*»** деб номланиб, унда кибержиноятлар объектига нисбатан содир этилишига қараб таснифланган шахснинг ҳаёти, соғлиғи, ахлоқи, ҳуқуқ ва манфаатларига қарши қаратилган кибержиноятлар, ижтимоий-сиёсий кибержиноятлар, иқтисодиёт соҳасидаги кибержиноятлар, ахборот-коммуникация технологияларига қарши қаратилган кибержиноятларнинг юридик тавсифи ёритиб берилган.

Ушбу бобнинг «*Шахснинг ҳаёти, соғлиғи, ахлоқи, ҳуқуқ ва манфаатларига қарши қаратилган кибержиноятларнинг юридик таҳлили*»га бағишланган биринчи параграфида кибертехнологиялар орқали ўзини ўзи ўлдириш даражасига етказиш жинояти, кибертехнологиялар орқали ўзини ўзи ўлдиришга ундаш-киберсуицид, кибертаҳдид, кибертехнологиялар орқали вояга етмаган шахсни ғайриижтимоий хатти-ҳаракатларга жалб қилиш, киберпорнография, киберзўравонлик, киберқўшмачилик, кибертуҳмат, киберҳақорат, кибертехнологиялар орқали шахсий ҳаёт дахлсизлигини бузиш, шахсга доир маълумотлар тўғрисидаги қонунчилик ҳужжатларини бузиш, хат-ёзишмалар, телефонда сўзлашув, телеграф хабарлари ёки бошқа хабарларнинг сир сақланиши тартибини бузиш, ахборот-коммуникация технологияларига нисбатан муаллифлик ёки ихтирочилик ҳуқуқларини бузиш каби кибержиноятларнинг жиноий-ҳуқуқий жиҳатларини тадқиқ қилиниб, уларнинг юридик тавсифи баён қилинган.

Диссертант томонидан ҳар бир жиноятлар халқаро ҳуқуқ нормалари ва хорижий мамлакатлар жиноят қонунчилиги билан ўзаро таҳлил қилиниб, мамлакатимизда олиб борилаётган ислоҳотлардан келиб чиқиб ҳамда мавжуд муаммоларнинг самарали ечими сифатида мазкур жиноятлар учун жавобгарликни белгилаш таклифи илмий асосланган.

«*Ижтимоий-сиёсий кибержиноятларнинг жиноий-ҳуқуқий таҳлили*» деб номланган ушбу бобнинг иккинчи параграфида кибертехнологиялар орқали урушни тарғиб қилиш, киберагрессия, кибертерроризм, киберэкстремизм, давлат раҳбарига ёки бошқа мансабдор шахсга нисбатан кибертажовуз, кибертехнологиялар орқали давлатларнинг конституциявий тузумига тажовуз қилиш, кибержосуслик, киберқўпорувчилик, кибертехнологиялар орқали давлат сирларини ошкор қилиш, киберпора, электрон ҳужжатларни қалбакилаштирганлик жинояти, кибербезорилик, киберқиморбозлик каби кибержиноятларнинг юридик тавсифи очиб берилган.

Шунингдек, тадқиқотчи томонидан ҳар бир жиноятлар халқаро ташкилотлар ва хорижий мамлакатлар жиноят қонунчилиги билан ўзаро таҳлил қилиниб, мамлакатимизда олиб борилаётган ислоҳотлардан келиб чиқиб ҳамда мавжуд муаммоларнинг самарали ечими сифатида мазкур жиноятлар учун жавобгарликни белгилаш таклифи илгари сурилган.

Ушбу бобнинг учинчи параграфи «*Иқтисодиёт соҳасидаги кибержиноятларнинг жиноий-ҳуқуқий тавсифи*» деб номланган бўлиб, унда кибертовламачилик, киберрастрата, киберфирибгарлик, киберўғрилик, сохта кибердоришунослик, кибертехнологиялардан фойдаланиб пул маблағларини ва (ёки) бошқа мол-мулкни жалб этишга доир ноқонуний фаолият кибержиноятларининг юридик тавсифи ишлаб чиқилган. Бунда, кибертовламачилик, киберрастрата, киберфирибгарлик, киберўғрилик, сохта кибердоришунослик, кибертехнологиялардан фойдаланиб пул маблағларини ва (ёки) бошқа мол-мулкни жалб этишга доир ноқонуний фаолият жиноятлари 16 ёшга тўлган ақли расо шахс томонидан содир этилиши асослантирилган, мазкур жиноятларнинг барчаси тўғри қасддан амалга оширилиши асослантирилган. Шу билан бир қаторда, ушбу жиноятларнинг объекти ва объектив томонлари таҳлил қилинган ҳамда мазкур жиноятларнинг юридик тавсифи диссертация ишида алоҳида жадвал кўринишида кўрсатиб берилган.

«*Ахборот-коммуникация технологияларига қарши қаратилган кибержиноятларнинг юридик таҳлили*» деб номланган тўртинчи параграфда Ўзбекистон Республикаси Жиноят кодексининг XX[1] боби бўлган ахборот технологиялари соҳасидаги жиноятлар, хусусан, Жиноят кодексининг 278[1]-моддасидаги ахборотлаштириш қоидаларини бузиш, 278[3]-моддасидаги компьютер тизимидан, шунингдек телекоммуникация тармоқларидан қонунга хилоф равишда (рухсатсиз) фойдаланиш учун махсус воситаларни ўтказиш мақсадини кўзлаб тайёрлаш ёхуд ўтказиш ва тарқатиш, 278[4]-моддасидаги компьютер ахборотини модификациялаштириш, 278[5]-моддасидаги компьютер саботажи, 278[6]-моддасидаги зарар келтирувчи дастурларни яратиш, ишлатиш ёки тарқатиш, 278[7]-моддасидаги телекоммуникация тармоғидан қонунга хилоф равишда (рухсатсиз) фойдаланиш жиноятларининг юридик тавсифи кўрсатиб берилган. Шу билан бирга жавобгарликни либераллаштириш зарурлиги, ушбу жиноятларнинг бир қисмини декриминаллаштириш ва маъмурий ҳуқуқбузарлик тоифасига ўтказилиши асосланган.

Бунда, диссертант томонидан ахборотлаштиришга оид қонунчилик ҳужжатларини бузиш, компьютер ахборотидан қонунга хилоф фойдаланиш, компьютер ахборотини модификациялаштириш, компьютер тизимидан, шунингдек телекоммуникация тармоқларидан қонунга хилоф равишда (рухсатсиз) фойдаланиш учун махсус воситаларни ўтказиш мақсадини кўзлаб тайёрлаш ёхуд ўтказиш ва тарқатиш, компьютер саботажи, зарар келтирувчи дастурларни яратиш, ишлатиш ёки тарқатиш, телекоммуникация тармоғидан қонунга хилоф равишда (рухсатсиз) фойдаланиш жиноятлари 16 ёшга тўлган ақли расо шахс томонидан содир этилиши асослантирилган, мазкур жиноятлардан ахборотлаштиришга оид қонунчилик ҳужжатларини бузиш, компьютер ахборотидан қонунга хилоф фойдаланиш, компьютер ахборотини модификациялаштириш жиноятлари эҳтиётсизлик (бепарволик ёки ўз-ўзига ишони) ва қасддан (тўғри қасд ёки эгри қасд), қолган компьютер тизимидан, шунингдек телекоммуникация тармоқларидан қонунга хилоф равишда

(рухсатсиз) фойдаланиш учун махсус воситаларни ўтказиш мақсадини кўзлаб тайёрлаш ёхуд ўтказиш ва тарқатиш, компьютер саботажи, зарар келтирувчи дастурларни яратиш, ишлатиш ёки тарқатиш, телекоммуникация тармоғидан қонунга хилоф равишда (рухсатсиз) фойдаланиш жиноятлари эса, тўғри қасддан амалга оширилиши асослантирилган ва тегишли таклиф-тавсиялар ишлаб чиқилган.

Илмий ишнинг ***«Кибержиноятлар учун жазо тайинлаш ва кибержиноятлар профилактикасини такомиллаштириш истиқболлари»***га оид учинчи боби кибержиноятлар учун жазо ва жавобгарлик масалалари, кибержиноятчиликка қарши курашиш, киберхавфсизликни таъминлаш, содир этилган кибержиноятларни экспертизадан ўтказиш, кибержиноятларни тергов қилиш ва кибержиноятчиликка қарши курашиш бўйича ваколатли органларни белгилаш ва мамлакатимизда киберхавфсизликни таъминлаш истиқболларига бағишланган.

Мазкур бобнинг биринчи параграфи «*Кибержиноятлар учун жазо тайинлашнинг ўзига хос хусусиятлари*» деб номланган бўлиб, унда туркумланган ва ушбу туркумга кирувчи асосий кибержиноятлар учун жазо тайинлашнинг ўзига хос хусусиятлари ёритилиб, кибержиноят содир этилиши натижасида келиб чиққан зарарни бартараф қилишнинг ҳуқуқий ва техник ечимлари, шу билан бирга, кибержиноятлар учун жазо тайинлаш вақтида кибержиноятларнинг вақт ва ҳудуд бўйича амал қилиш доирасини, шунингдек, келиб чиққан ҳақиқий зарарни аниқлаш бўйича мавжуд муаммоларни ҳал этиш тартиби илмий асосланган. Шунингдек, Озарбайжон, Болгария, Грузия, Филиппин каби давлатларнинг жиноят қонунчилигида кибержиноятлар учун жазо тайинлаш механизми ўрганилган.

Натижада, муаллиф таклифлари асосида Ўзбекистон Республикаси Жиноят кодекси моддалари қайта кўриб чиқилиб, ушбу кодекснинг 130-130^{1}, 139-140, 141^{1}-141^{2}, 158, 244, 244^{1}, 244^{5}-244^{6}-моддаларига тегишли ўзгартиш ва қўшимчалар киритилиб, Интернет ва телекоммуникация воситалари орқали бир қатор ижтимоий хавфли қилмишларни содир этганлик учун жавобгарлик белгиланган, мавжуд жавобгарлик кучайтирилган.

Тадқиқотчининг фикрига кўра, ахборот технологиялари ва коммуникациялари орқали ҳимояланган ижтимоий муносабатлар кибержиноятларнинг объектини ташкил этади ва мазкур ижтимоий муносабатларга қилинган ҳужум тавсифи кибержиноятларнинг объектив томонини кўрсатади. Кибержиноятчиликнинг турлари ва шакллари турлича бўлганлиги сабабли ҳам унинг объектив томонини аниқ кўрсатиш мураккаб ва ҳар бир кибержиноятнинг тури бўйича объектив томон жиноят содир этилиши шаклига қараб турлича ифодаланади.

«*Кибержиноятлар профилактикасини такомиллаштириш истиқболлари*» деб номланган иккинчи параграфда кибержиноятларнинг олдини олиш, уларга қарши курашиш ва профилактикаси бўйича мамлакатимиз олдида турган вазифалар санаб ўтилиб, уларни амалга ошириш механизми ишлаб чиқилган. Шунингдек, мазкур йўналишда

қўйилган вазифаларни амалга ошириш учун давлат органларининг ваколатлари аниқ белгилаб қўйилиши халқаро ва хорижий тажриба нуқтаи назаридан асосланган.

Тадқиқотчининг таъкидлашича, Cybersecurity Ventures халқаро экспертларнинг фикрига кўра, дунё бўйлаб ҳар ҳар 14 сонияда битта киберҳужум содир этилмоқда, Жаҳон иқтисодий форумининг прогнозига кўра, киберҳужумлар натижасида 2022 йилда дунё 8 трлн. доллар миқдорида зарар кўради. Ушбу зарарни бартараф этиш бўйича кибержиноятларнинг олдини олиш борасида олимлар турлича тушунтириш беришга ҳаракат қилиб кўради, хусусан, олим В.С.Харламов, Я.Попыева, М.А.Ефремованинг фикрича, ушбу муаммонинг ягона ечими кибержиноятчилик тушунчасини мамлакат жиноят қонунчилигига киритиш керак.

Диссертант томонидан Болгария жиноят кодексининг 319^{a}-319f-моддалари, Грузиянинг жиноят кодексининг 284-286-моддалари, Белеруссия жиноят кодексининг 24-бобининг 1-изоҳ қисми, Дания жиноят кодексининг 279-а-моддасида, Франция жиноят кодексининг 263а-моддасида, Эстония жиноят кодексининг 268-моддасида компьютер фирибгарлиги, Италия жиноят кодексининг 640-ter-моддасида, Хитой Халқ Республикаси Жиноят кодексининг 287-моддасида, Нидерландия Жиноят кодексининг 138ab-моддасининг «а» бандининг учинчи хатбошиси, Польша Жиноят кодексининг 287-моддасида, Украина Жиноят кодексининг 190-моддаси 3-қисми, Жанубий Корея Жиноят кодексининг 247^{2}-моддасида, Испания Жиноят кодексининг 478-моддасида, Финландия Жиноят кодексининг 30-боби 4-моддаси 1-бандида, Швейцария Жиноят кодексининг 143-моддасида, Австрия Жиноят кодексининг 148а-моддасидаги кибержиноятларга оид нормалар мавжудлигидан келиб чиқиб, Ўзбекистон Республикаси Жиноят кодексини такомиллаштиришга оид таклифлар берилган.

Мамлакатда киберхавфсизликни таъминлашнинг энг самарали усули сифатида киберхавфсизлик бўйича стратегия қабул қилиш ҳисобланади. Хорижий давлатлардан Украина, АҚШ, Эстония, Литва, Испания, Германия, Словакия, Япония, Швейцария, Норвегия, Янги Зеландия, Ҳиндистон, Австралия, ЖАР, Канада, Финландия, Австрия, Руминия, Полша, Франция, Чехия, Нидерландия, Люксембург каби давлатларда бу каби стратегиялар қабул қилинган. Шундан келиб чиқиб, Ўзбекистон Республикаси Президентининг 2020 йил 2 мартдаги ПФ–5953-сон Фармони билан тасдиқланган «2017-2021 йилларда Ўзбекистон Республикасини ривожлантиришнинг бешта устувор йўналиши бўйича Ҳаракатлар стратегиясини «Илм, маърифат ва рақамли иқтисодиётни ривожлантириш йили»да амалга оширишга оид давлат дастурининг 243-бандида 2020-2023 йилларга мўлжалланган киберхавфсизликка доир миллий стратегияни ишлаб чиқиш белгиланган ва унинг ижроси сифатида имкон қадар тезроқ киберхавфсизлик бўйича стратегия қабул қилиш мақсадга мувофиқлиги асосланган.

Киберхавфсизликни таъминлашда энг катта тахдид, давлат органлари ва идораларининг лоқайдлиги ҳисобланади. Тан олиш керакки, аксарият вазирлик ва идоралар, корхоналар рақамли технологиялардан мутлақо йироқ. Шу сабабдан ҳам лоқайдликка барҳам бериш орқали киберхавфсизликни таъминлаш учун зарур давлат дастурлари ва йўл-хариталарини ишлаб чиқиб, уларни ҳаётга татбиқ қилиш асосланган.

ХУЛОСА

Кибержиноятларнинг жиноий-ҳуқуқий жиҳатларини комплекс тадқиқ этиш бўйича қуйидаги илмий-амалий таклиф ҳамда тавсиялар ишлаб чиқилди:

I. Жиноят ҳуқуқи фанини ривожлантириш бўйича илмий-назарий хулосалар:

1. Кибержиноят, кибержиноятчилик ва кибертехнологиялар тушунчаларига қуйидагича муаллифлик таърифлари ишлаб чиқилди:

кибержиноят – ахборот-коммуникация технологияларидан фойдаланиб ёки уларга нисбатан амалга ошириладиган, Жиноят Кодекси билан тақиқланган ва жазо қўллаш белгиланган кибермуҳитда содир этиладиган айбли ижтимоий хавфли қилмиш (ҳаракат ёки ҳаракатсизлик);

кибертехнологиялар – ахборот-коммуникация технологиялари, рақамли технологиялар, кибертехнологиялар, робототехника, дастурий маҳсулотлар, дастурий-аппарат маҳсулотлар, телекоммуникация воситалари, алоқа объектлари, компьютер тизими, телекоммуникация, Интернет, алоқа ва бошқа тармоқлар, тизимлар, ахборот ресурси, ахборот тизими, маълумотлар базаси ва бошқа технологиялар жами.

2. Кибержиноятларнинг ҳозирги кунда 200 дан ортиқ тури бўлиб, уларни таснифлаш орқали ўрганиш мақсадга мувофиқдир. Кибержиноятларни қуйидаги гуруҳларга ажратиб ўрганиш мумкин:

кибержиноятлар амалга ошириш усулига кўра, иккита катта гуруҳга бўлинади, кибертехнологиялардан фойдаланиб содир этиладиган кибержиноятлар ва кибертехнологияларга қарши қаратилган кибержиноятлар. Буни аниқроқ тушунтирадиган бўлсак, кибержиноятлар ахборот-коммуникация технологияларидан фойдаланиб содир этиладиган кибержиноятларга ва ахборот-коммуникация технологияларига нисбатан содир этиладиган жиноятларга бўлинади. Жиноят кодексининг 103-моддасининг иккинчи қисми «г»-банди, 103^1-моддасининг иккинчи қисми «в»-банди, 167-моддасининг учинчи қисми «г»-банди, 168-моддасининг иккинчи қисми «в»-банди, 169-моддасининг учинчи қисми «б»-банди, 188^1, 244^1, 244^5 ва 278-моддаларида назарда тутилган ижтимоий хавфли қилмишлар ахборот-коммуникация технологияларидан фойдаланиб, Жиноят кодексининг 278^1-278^7-моддаларида назарда тутилган ижтимоий хавфли қилмишлар ахборот-коммуникация технологияларига нисбатан содир этилган кибержиноятлар саналади;

кибержиноятларни ижтимоий хавфли қилмишни қайси маконда содир этилишига қараб иккита гуруҳга ажратиш мумкин, яъни ахборот-коммуникация технологиялари соҳасига тегишли кибермаконда содир этиладиган кибержиноятлар ва ахборот соҳасида содир этиладиган кибержиноятлар. Иккала жиноят ҳам кибермуҳитда содир этилади, бироқ ахборот-коммуникация технологиялари соҳасидаги кибержиноятларда ахборот-коммуникация технологияси зарар кўриши ёки зарар етадиган

ҳолатга олиб келиниши мумкин. Ахборот соҳасидаги кибержиноятларда эса, ахборот-коммуникация технологияларига зарар етмайди, балки фойдаланувчиларга зарар етказувчи маълумотлар уларнинг ахборот-коммуникация технологиясида сақланиши, узатилиши ва фойдаланиши орқали шахс, жамият ва давлат манфаатларига путур етказилади;

кибержиноятлар объектига нисбатан содир этилишига қараб, шахснинг ҳаёти, соғлиғи, ахлоқи, ҳуқуқ ва манфаатларига қарши қаратилган, ижтимоий-сиёсий, иқтисодиёт соҳасидаги, ахборот-коммуникация технологияларига қарши қаратилган кибержиноятларга бўлинади.

Барча кибержиноятлар кибермуҳитда содир этилади.

II. Ўзбекистон Республикасининг жиноят тўғрисидаги қонунчилигини такомиллаштиришга қаратилган таклифлар:

1. «Норматив-ҳуқуқий ҳужжатлар тўғрисида»ги Ўзбекистон Республикаси Қонуни талабига асосан, Ўзбекистон Республикаси Жиноят кодексининг VIII бобига ахборот-коммуникация технологиялари, рақамли технологиялар, кибертехнологиялар, кибержиноят, кибержиноятчилик, киберҳуқуқбузарлик, киберхавфсизлик, кибертехнологиялар орқали ёки уларга нисбатан содир этиладиган кибержиноятларнинг тушунчалари мазмун-моҳиятини киритиш ҳамда тадқиқот ишида кўриб чиқилган шаклда мазкур тушунчаларнинг амалга ошириш механизмини белгиловчи тадқиқот ишининг 1-иловасида назарда тутилган Жиноят кодексининг 103, 103^1, 112, 127, 130-131, 139-140, 141^1-141^2, 149-150, 155^1, 156, 158-159, 162, 167, 167^1, 169, 186^3, 188^1, 228, 278, 278^1-278^7-моддаларини таҳрир ва кўринишда қайта кўриб чиқиш ҳамда Жиноят кодексини 143^3, 151^1, 160^1, 161^1, 165^1, 244а, 168^1, 169^1, 277^1-моддалар билан тўлдириш таклиф қилинади. Хусусан, муаллифнинг таклифлари асосида Ўзбекистон Республикасининг Жиноят кодекси қайта кўриб чиқилиб, Жиноят кодексининг 130-130^1-, 139-140-, 150-, 244-244^1, 244^5-244^6-моддалари қайта кўриб чиқилиб, порнографик ва зўравонликни тарғиб қилувчи маҳсулотни телекоммуникация тармоқларида ёки Интернет жаҳон ахборот тармоғида реклама қилиш, намойиш этиш, тарқатиш, телекоммуникация тармоқларида ёки Интернет жаҳон ахборот тармоғида жойлаштириш орқали туҳмат қилиш ва ҳақорат қилиш, Ўзбекистон Республикаси Президентини телекоммуникация тармоқларидан ёки Интернет бутунжаҳон ахборот тармоғидан фойдаланган ҳолда уни ҳақоратлаш ёки унга туҳмат қилиш, телекоммуникациялар тармоқларидан, Интернет жаҳон ахборот тармоғидан фойдаланган ҳолда оммавий тартибсизликларга ва фуқароларга нисбатан зўравонлик қилишга омма олдида даъват қилиш, жамоат хавфсизлиги ва жамоат тартибига таҳдид соладиган материалларни, шунингдек, карантинли ва инсон учун хавфли бўлган бошқа юқумли касалликларнинг пайдо бўлиши ҳамда тарқалиши шароитида карантинли ва инсон учун хавфли бўлган бошқа юқумли касалликлар тарқалиши ҳақида ҳақиқатга тўғри келмайдиган маълумотларни, шахснинг қадр-қиммати камситилишига ёки унинг обрўсизлантирилишига

олиб келадиган ёлғон ахборотни тарқатиш учун жиноий жавобгарлик белгиланди;

2. Ўзбекистон Республикасининг «Киберхавфсизлик тўғрисида»ги Қонунини қабул қилиш таклиф қилинади ва унинг лойиҳаси ишлаб чиқилиб, диссертациянинг 2-иловасида тақдим қилинган;

3. Ўзбекистон Республикасининг «Киберагрессия тўғрисида» ҳамда «Кибержиноятларга қарши курашиш тўғрисида»ги Қонунларини қабул қилиш таклиф қилинади (қонуннинг тузилиши ишлаб чиқилган).

III. Суд амалиёти ва жиноятчиликка қарши курашиш тизими самарадорлигини оширишга қаратилган тавсиялар:

1. Киберхавфсизликни таъминлаш, кибержиноятлар профилактикасини ташкил этиш борасидаги ишларни тизимлаштириш мақсадида Ўзбекистон Республикасининг «Киберхавфсизлик тўғрисида», «Кибержиноятчиликка қарши курашиш тўғрисида», «Киберагрессия тўғрисида»ги қонунлари асосида уларнинг ижросини таъминлаш учун зарур бўлган чора-тадбирлар ишлаб чиқиш;

2. Киберхавфсизликни лозим даражада таъминлаш мақсадида қуйидаги чора-тадбирларни амалга ошириш мақсадга мувофиқ:

1) ахборот ресурслари ва ахборот тизимларини муҳофаза қилиш тартиби бўйича ягона норматив-ҳуқуқий ҳужжат ҳали хануз ишлаб чиқилмаган, ваҳоланки, ахборот ресурслари ва ахборот тизимларининг ҳуқуқий режими маазкур ҳолатни белгиловчи нормалар билан аниқланиши 2003 йилдаёқ қонунчилик ҳужжатларимизда кўрсатиб қўйилган эди. Шунга биноан, ахборот ресурслари ва ахборот тизимларининг ҳуқуқий режимини акс этувчи ягона ҳужжат ишлаб чиқиш, мазкур ҳужжатда ахборот ресурслари ва ахборот тизимлари, ҳимояланган тизим ҳуқуқий ҳолати, ахборот-коммуникация технологиялари, тизими, тармоғи, муҳофазаси каби тушунчаларнинг ягона таърифи, уларни қўллаш механизми, ахборот-коммуникация технологиялари, тизими ва тармоғига кирувчи технологияларнинг ягона реестри белгилаб қўйиш;

2) Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлиги топшириғига мувофиқ телекоммуникация оператори ва провайдерлари орқали бепул, солиқ ҳисобланмайдиган смс-хабарномаларни йўллаш амалиётини ташкил қилиш ва унда соҳага оид қонун ҳужатлари билан аҳолининг барча қатламларини таништириб бориш, киберхавф-хатарлар ҳақида уларни ўз ақтида лозим даражада огоҳлантириш чораларини кўриш;

3) оила-мактабгача таълим-мактаб-коллеж-лицей-олий ўқув юрти-ишхона-оила режимини йўлга қўйиш орқали ахборот-коммуникация технологиялари соҳасини босқичма-босқич ўргатиш чораларини кўриш;

4) давлат бюджетини шакллантириш вақтида киберхавфсизликни таъминлашга қаратилган харажатларни алоҳида сметада кўрсатиб ўтиш;

5) ахборот-коммуникация технологиялари соҳасини ўқитиш, кадрлар тайёрлаш ва кадрлар малакасини ошириш бўйича тизимли ишларни ривожлантириш;

6) ахборот-коммуникация технологиялари ҳуқуқи, кибержиноятчилик ҳуқуқи, киберхавфсизликни таъминлаш асослари каби ўқув дастури ва фанларни мактабгача таълим-мактаб-коллеж-лицей-олий ўқув юрти кесимида ўқитиш чораларини кўриш;

7) кибержиноятлар ва киберҳуқуқбузарликлар натижасида келиб чиққан зарарни аниқлаш, ҳисоб-китоб қилиш, ундириш методикасини ишлаб чиқиш ва қабул қилиш;

8) халқаро ташкилотлар ва хорижий давлатлар билан ялпи ҳамкорлик қилиш мақсадида дастлаб 2001 йилдаги Будапешт конвенциясига қисман аъзо бўлиш ва кейинчалик кибержиноятчилик ва киберҳуқуқбузарликка қарши ялпи курашувчи, давлатларда киберхавфсизликни таъминловчи ягона халқаро ҳужжатни ишлаб чиқиш ва барча дунёдаги давлатлар томонидан уни қабул қилиш орқали Будапешт конвенциясидан чиқиш масаласини кўриб чиқиш;

9) таълим соҳасида кибержиноятчилик, киберҳуқуқбузарлик ва киберхавфсизлик бўйича ҳам ҳуқуқшунослик, ҳам техник билим бериш орқали ягона ахборот-коммуникация технологиялари соҳасида ҳуқуқшунос-техник кадрларни тайёрлаш тизимини йўлга қўйиш;

10) аҳолининг хусусий мулки бўлган телефон, компьютер ва бошқа технологиялари орқали унинг хусусий мулкига бўлаётган ёки бўлиши кутилаётган киберҳужумлар ҳақида маълумот бериш имкониятларини яратиш ва амалда қўллаш;

11) кибержиноятчилар ва киберҳуқуқбузарликка йўл қўйган шахслар орасидан давлатнинг киберхавфсизлигини таъминлаш бўйича махсус билимга эга бўлган шахсларни давлат манфаатлари учун хизмат қилиш орқали унга нисбатан қўлланилган жазодан озод қилиш, аммо келтирилган зарарни қоплаш имкониятини бериш тизимини яратиш ва амалиётга жорий қилиш;

12) Жиноят-процессуал қонунчилигимини такомиллаштириш, далилларнинг мақбуллигини таъминлаш ва лозим даражада тергов харакатларини олиб бориш мақсадида ахборот-коммуикация технологиялари ва кибертехнологиялар орқали ёки уларга нисбатан содир этилган жиноятларни тергов қилишга оид Ўзбекистон Республиркаси Олий суди Пленуми тушунтириш бериши бўйича қарорини қабул қилиш;

13) киберхавфсизликни таъминлаш соҳасидаги мавжуд муаммоларнинг ечимини ҳал қилишга қаратилган илмий тадқиқот ишлари доирасини янада кенгайтириш ва мунтазам йўлга қўйиш кабилардан иборат.

НАУЧНЫЙ СОВЕТ DSc.32/30.12.2020.Yu.74.01 ПО ПРИСУЖДЕНИЮ УЧЕНЫХ СТЕПЕНЕЙ ПРИ УНИВЕРСИТЕТЕ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ УЗБЕКИСТАН

УНИВЕРСИТЕТ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ УЗБЕКИСТАН

АНОРБОЕВ АМИРИДДИН УЛУҒБЕК УГЛИ

УГОЛОВНО-ПРАВОВЫЕ АСПЕКТЫ КИБЕРПРЕСТУПЛЕНИЙ

12.00.08 – Уголовное право. Криминология. Уголовно-исполнительное право

АВТОРЕФЕРАТ
диссертации доктора философии (PhD) по юридическим наукам

Ташкент – 2021

Тема диссертации доктора философии (PhD) зарегистрирована в Высшей аттестационной комиссии при Кабинете Министров Республики Узбекистан № B2019.1.PhD/Yu274.

Диссертация выполнена в Университете общественной безопасности Республики Узбекистан.

Автореферат диссертации размещен на трех языках (узбекском, русском и английском) на веб-сайтУниверситета общественной безопасности Республики Узбекистан (www.mgjxu.uz) и информационно-образовательного портала «Ziyonet» (www.ziyonet.uz).

Научный руководитель:	**Рустамбаев Мирзаюсуп Хакимович** доктор юридических наук, профессор
Официальные оппоненты:	**Инагамджанова Зумратхон Фатхуллаевна** доктор юридических наук, профессор
	Расулев Абдулазиз Каримович доктор юридических наук, профессор
Ведущая организация:	**Академия Генеральной Прокуратуры Республики Узбекистан**

Защита диссертации состоится «27» ноября 2021 года в 10-00 часов на заседании Научного совета DSc. 32/30.12.2020.Yu/74.01 по присуждению ученых степеней при Университете общественной безопасности Республики Узбекистан. (Адрес: 100109, Ташкентская обл., Зангиотинский район, поселок Чорсу. Тел.: (99871) 230-32-71; факс: (99871) 230-32-50; mgjxu@umail.uz).

С диссертацией можно ознакомится на Информационно-ресурсном центре Университета общественной безопасности Республики Узбекистан (зарегистрирован за № 2166/1). (Адрес: 100109, Ташкентская обл., Зангиотинский район, поселок Чорсу. Тел.: (99871) 230-32-71; факс: (99871) 230-32-50).

Автореферат диссертации разослан «12» ноября 2021 года.

(Реестр протокола рассылки № 9 от «12» ноября 2021 года).

Миразов Д.М.
Заместитель председателя научного совета по присуждению ученых степеней, доктор юридических наук, профессор

Нурматов М.М.
Ученый секретарь научного совета по присуждению ученых степеней, доктор юридических наук, доцент

Усмонов М.Б.
Председатель научного семинара при научном совете по присуждению ученых степеней, доктор юридических наук, профессор

ВВЕДЕНИЕ (аннотация диссертации доктора философии (PhD)

Актуальность и востребованность темы диссертации. Во всем мире одним из самых опасных деяний, причиняющих вред информационным системам и ресурсам государств, базам данных международных организаций и компаний, информационно-коммуникационным технологиям финансовых учреждений, а также правам и интересам человека, являются киберпреступления. Так, по мнению экспертов международной организации Cybersecurity Ventures, анализирующей киберпреступления, «каждые 14 секунд по всему миру происходит одна кибератака, в результате которого, по прогнозам Всемирного экономического форума, в 2022 году страны мира могут понести ущерб в размере 8 триллионов долларов»[1]. Поэтому на сегодняшний день, для предотвращения этой опасности, борьбы с ней и устранения причин ее возникновения, разработка эффективных механизмов борьбы с киберпреступлениями, а также создание комплексных основ обеспечения кибербезопасности имеет первостепенное значение для отрасли уголовного права.

В мире осуществляются научные исследования по обеспечению кибербезопасности исходя из того, что киберпреступления имеют гораздо более широкий характер по сравнению с иными преступлениями, они могут находясь в одной стране совершаться на территории другой страны, являются трансграничным преступлением, для киберпреступников их совершение экономически выгодно, и с точки зрения времени имеет оперативный характер, возможно причинение материального и морального вреда в особо крупном размере, а также наличие в данной сфере системных недостатков касательно организационно-правовых механизмов. В настоящее время для всех государств мира приоритетной задачей является пересмотр нормативно-правовых актов, определяющих ответственность за киберпреступления в национальных и международных уголовно-правовых отношениях, необходимость взаимной гармонизации международных норм по кибербезопасности с национальным законодательством, создание механизма всеобщей борьбы с данными преступлениями посредством унификации уголовного законодательства государств о киберпреступности, налаживание международного сотрудничества и партнерских отношений по обеспечению кибербезопасности, поиск эффективных научно-теоретических и практических решений, а также научный анализ обеспечения кибербезопасности.

В нашей республике последовательно осуществляются масштабные программные мероприятия по приоритетным направлениям обеспечения верховенства закона и дальнейшего реформирования судебно-правовой системы. В Стратегии действий по пяти приоритетным направлениям развития Республики Узбекистан на 2017-2021 годы определены такие важные задачи, как «совершенствование и либерализация норм уголовного и

[1] https://www.tadviser.ru.

уголовно-процессуального законодательства, декриминализация отдельных уголовных деяний, гуманизация уголовных наказаний и порядка их исполнения; повышение эффективности координации деятельности по борьбе с преступностью и профилактике правонарушений; усиление организационно-практических мер по борьбе с религиозным экстремизмом, терроризмом и другими формами организованной преступност»[1]. Это свидетельствует о необходимости изучения причин и факторов возникновения киберпреступлений, юридического анализа киберпреступлений и проведения необходимых научных исследований по предупреждению подобных общественно опасных деяний.

Диссертационная работа в определенной степени послужит реализации задач, предусмотренных в Указах Президента Республики Узбекистан от 7 февраля 2017 года №УП–4947 «О Стратегии действий по дальнейшему развитию Республики Узбекистан», от 13 июля 2018 года №УП–5482 «О мерах по дальнейшему совершенствованию судебно-правовой системы и повышению доверия к органам судебной власти», постановлений Президента Республики Узбекистан от 14 мая 2018 г. № ПП–3723 «О мерах по кардинальному совершенствованию системы уголовного и уголовно-процессуального законодательства» и от 3 сентября 2020 г. №ПП–4818 «О мерах по цифровизации деятельности органов судебной власти», постановления Кабинета Министров от 7 августа 2018 г. № 622 «Об утверждении Концепции активизации деятельности органов государственного и хозяйственного управления в виртуальном пространстве» и других законодательных актах в этой сфере.

Соответствие исследования приоритетным направлениям развития науки и технологий республики. Исследование выполнено в соответствии с приоритетным направлением развития науки и техники «III. Подготовка высококвалифицированных научных и инженерных кадров и их ориентация на научную деятельность».

Степень изученности проблемы. Следует отметить, что в Республике Узбекистан вопросы, касательно борьбы с киберпреступлением борьбой и обеспечением кибербезопасности, недостаточно комплексно изучены, а исследованы лишь некоторые ее аспекты. В частности, И.Р.Бегишев исследовал кибермошенничество, Х.Р.Очилов – меры ответственности за хищение чужого имущества с использованием компьютерных средств, Ш.Гойибназаров, И.И.Аминов, М.М.Мирхаётов – кибертерроризм и преступления, связанные с финансированием кибертерроризма, А.А.Исманова – киберэкстремизм, И.М.Норбутаев – преступления против общественного порядка, Н.Раджабова – преступления в виде доведения до самоубийства и (или) склонения к самоубийству посредством информационно-коммуникационных технологий, А.К.Расулев – пути совершенствования уголовно-правовых и

[1] Указ Президента Республики Узбекистан «О Стратегии дальнейшего развития Республики Узбекистан» от 7 февраля 2017 года № УП–4947 // lex.uz - Национальная база данных законодательства Республики Узбекистан.

криминологических мер борьбы с преступностью в сфере информационных технологий и безопасности, У.Ф.Хасанов – преступления в виде незаконного (несанкционированного) использования компьютерной информации, А.Хаджаев, Н.Юсупова – пути борьбы с компьютерной преступностью, Д.Р.Иргашев, М.А.Рахматуллаев – состояние повышения безопасности данных блокчейна. Российскими учеными также были проведены исследования, в частности К.Н. Евдокимов – компьютерную преступность России, Т.Л. Тропина – преступления компьютерного саботажа, Р.И. Дремлюга – преступления, совершаемые через Интернет, В.В. Хилюта – преступления в виде киберграбежей, Е.В. Тищенко – особенности уголовной ответственности за компьютерные преступления или Интернет-преступность, В.О. Голубев – проблемы противодействия транснациональной компьютерной преступности, С.И. Ушаков – практические и теоретические положения преступлений в сфере компьютерной информации, Е.Щербак и Н. Щербак – особенности квалификации компьютерной преступности, А.А. Данельян – международно-правовые аспекты создания безопасного киберпространства[1].

Комплексные исследования в сфере борьбы с киберпреступностью и обеспечением кибербезопасности осуществлялись М. Маклюэн (Канада), Т.Стоуньер (Великобритания), Й. Масуда (Япония), R.Haeni, F.Schreier, B.Weekes, T.H.Winkler (Германия) и другими. Кроме того, вопросы кибербезопасности изучались Nationales Cyber-Abwehrzentrum-NCAZ (Германия), Australian Cyber Security Center-ACSC (Австралия), National Cyber Security Centre (Ирландия), National Cybersecurity Center-NCSC (Буюк Британия), Национальным координационным центром по компьютерным инцидентам-НКЦКИ (Россия), National Cybersecurity Center-NCSC (США), а в Узбекистане государственным унитарным предприятием «Центр кибербезопасности», организованный постановлением Президента Республики Узбекистан от 14 сентября 2019 года №ПП–4452 «О дополнительных мерах по совершенствованию системы контроля за внедрением информационных технологий и коммуникаций, организации их защиты».

Связь темы диссертации с планом научно-исследовательских работ высшего образовательного учреждения, в котором выполнена диссертация. Тема диссертации реализована в рамках «Плана по устранению причин и условий, способствующих совершению преступности и правонарушений в Военно-техническом институте Национальной гвардии Республики Узбекистан».

Цель исследования состоит в анализе уголовно-правовых аспектов киберпреступлений, разработке научно-практических предложений и рекомендаций по обеспечению кибербезопасности.

Задачи исследования:

раскрытие понятия киберпреступления и его сущности;

[1] Полный список работ этих ученых приведен в списке использованной литературы диссертации.

изучение необходимости систематизации в уголовном законодательстве ответственности за киберпреступления;

анализ киберпреступлений посредством их классификации;

юридический анализ киберпреступлений, направленных против жизни, здоровья, нравственности, прав и интересов человека;

анализ социально-политических киберпреступлений;

анализ киберпреступлений в сфере экономики;

раскрытие юридического анализа киберпреступлений, направленных против информационно-коммуникационных технологий;

анализ особенностей назначения наказаний за киберпреступления;

определение перспектив совершенствования профилактики киберпреступлений, а также разработка предложений и рекомендаций по совершенствованию законодательства.

Объект исследования составляют общественные отношения, связанные с правовым регулированием уголовно-правовых аспектов киберпреступлений в Республике Узбекистан.

Предмет исследования составляют теоретико-правовой анализ киберпреступлений, юридический анализ киберпреступлений, вопросы, связанные с назначением наказаний за киберпреступления и перспективами совершенствования профилактики киберпреступлений.

Методы исследования. В ходе исследования применены такие методы исследования, как анализ, синтез, дедукция, индукция, сравнительно-правовой анализ, исторический, анкетирование, анализ эмпирических материалов и статистических данных, наблюдение, системный и логический подход.

Научная новизна исследования состоит в следующем:

обосновано внедрение механизма проведения обязательной экспертизы программного обеспечения, баз данных, в том числе операционных систем государственных органов и организаций на соответствие требованиям информационной и кибербезопасности;

обосновано, что при обнаружении в текстах комментариев, оставленных пользователями веб-сайта, а также в социальных сетях или мессенджерах информации, ограниченной Министерством по развитию информационных технологий и коммуникаций Республики Узбекистан, Центром по вопросам массовых коммуникаций Республики Узбекистан Агентства информации и массовых коммуникаций при Администрации Президента Республики Узбекистан владельцу веб-сайта, веб-сайта и (или) страницы мессенджера, а также блоггеру направляется уведомление об удалении информации, запрещенной к распространению законодательством Республики Узбекистан;

обосновано определение уголовной ответственности за распространение не соответствующих действительности сведений о распространении карантинных и других опасных для человека инфекций в условиях возникновения и распространения карантинных и других опасных для человека инфекций в печатном или иным способом размноженном тексте

либо в средствах массовой информации, а также во всемирной информационной сети Интернет;

обосновано введение уголовной ответственности за изготовление или ввоз на территорию Республики Узбекистан с целью распространения, рекламирования, демонстрации, а равно рекламирование, демонстрация, распространение порнографической, пропагандирующей культ насилия или жестокости продукции, в том числе рекламирования, демонстрации, распространения в средствах массовой информации, сетях телекоммуникаций или во всемирной информационной сети Интернет.

Практические результаты исследования заключаются в следующем:

предложения об определении Службы государственной безопасности в качестве уполномоченного органа в сфере регулирования кибербезопасности служат внедрению и развитию в органах государственного и хозяйственного управления, органах государственной власти на местах, других организациях и ведомствах информационно-коммуникационных технологий на основе единого технологического подхода, а также осуществления контроля, мониторинга, изучения и проверки состояния информационной безопасности;

предложения об открытии направления образования по сфере кибербезопасности в высших образовательных учреждениях на ступени бакалавриата, а также налаживании системы подготовки кадров послужит подготовке высококвалифицированных специалистов по направлениям информационных технологий и кибербезопасности;

предложения по сфере информационно-коммуникационных технологий послужат определению полномочий проведения обязательной экспертизы проектов государственных органов и организаций по созданию и внедрению информационных систем, ресурсов и других программных продуктов в рамках развития цифровой экономики и электронного правительства, а также проектов нормативно-правовых актов в области в Министерстве по развитию информационных технологий и коммуникаций Республики Узбекистан, кроме того определению в качестве одной из основных задач и функций государственного учреждения «Центр управления проектами электронного правительства» обеспечения единого технологического подхода при реализации проектов электронного правительства и цифровой экономики, в том числе проведения комплексной экспертизы проектно-технической документации;

предложения по совершенствованию системы обучения кадров в сфере информационной безопасности, кибербезопасности и общественной безопасности, организации международного сотрудничества в сфере информационной и кибербезопасности, обеспечению общественного порядка и защиты персональных данных, расширению взаимовыгодного сотрудничества с международными организациями и зарубежными странами, организации реализации государственной политики в сфере обеспечения кибербезопасности информационных ресурсов и систем органов государственного и хозяйственного управления, местных исполнительных

органов, определению полномочий Кабинета Министров по принятию мер для сохранения целостности национального информационного пространства, послужат обеспечению полноценной реализации основных задач Департамента Кабинета Министров по вопросам развития IT-технологий, телекоммуникаций и инновационной деятельности;

предложения о разработке и принятии национальной стратегии кибербезопасности на среднесрочный период и проекта Закона Республики Узбекистан «О кибербезопасности» послужат урегулированию отношений в данной сфере единым законодательным актом.

Достоверность результатов исследования Достоверность результатов исследования объясняется получением примененных в работе методов, использованных в его рамках теоретических подходов из официальных источников, проведением взаимного анализа зарубежного опыта и актов национального законодательства, внедрением в практику выводов, предложений и рекомендаций, утверждением полученных результатов уполномоченными структурами. Вместе с тем, в рамках исследования были направлены запросы в 485 государственных органов и ведомств, образовательных учреждений, по результатам опроса, выявлено, что 438 работников 485 организаций не в достаточной степени имеют необходимые навыки и знания о киберпреступлениях и кибербезопасности, в организациях не имеется и материально-технической базы для обеспечения кибербезопасности, на основе материалов, полученных из иных организаций, было обогащено содержание диссертации.

Научная и практическая значимость результатов исследования. Научная значимость диссертации заключается в том, что выводы, предложения и рекомендации исследования обогащают теоретические знания уголовного права и создают возможности для проведения новых научных исследований, также его научно-теоретические идеи и выводы имеют научное значение для более глубокого изучения вопросов, связанных с совершенствованием экономико-правового механизма уголовного законодательства Республики Узбекистан.

Практическая значимость исследования заключается в том, что научные положения, выводы и рекомендации, сформулированные в результате исследования темы, послужат при разработке проектов законов Республики Узбекистан «О противодействии киберпреступлениям», «О кибербезопасности», «О киберагрессии», а также совершенствовании Уголовного кодекса Республики Узбекистан. Материалы исследования могут быть использованы в учебном процессе высших юридических образовательных учреждений при проведении лекций и семинаров по предметам «Уголовное право», «Уголовный процесс», «Криминалистика», «Цифровая криминалистика», «Гражданское право», «Кибернетика», «Информатика», «Информационное право».

Внедрение результатов исследования. На основе результатов исследования уголовно-правовых аспектов киберпреступлений:

предложение о внедрении системы обязательной экспертизы информационных систем всех государственных органов и организаций республики на соответствие требованиям информационной и кибербезопасности нашло свое отражение в пункте 28 Дорожной карты по реализации Стратегии «Цифровой Узбекистан – 2030» в 2020 — 2022 годах, утвержденной Указом Президента Республики Узбекистан от 5 октября 2020 г. №УП–6079 *(Акты Министерства по развитию информационных технологий и коммуникаций от 16.07.2020 г. № 32-8/4040, от 18.02.2021 г. №32-8/1190 и от 26.02.2021 г. № 32-8/1451).* Принятие этого предложения послужило обеспечению кибербезопасности информационных систем государственных органов и организаций путем проведения их обязательной экспертизы;

предложение о необходимости определения порядка направления уведомления владельцу веб-сайта, и (или) страницы мессенджера, а также блоггеру об удалении информации, запрещенной к распространению законодательством Республики Узбекистан нашло свое отражение в пункте 2 и приложении к Постановлению Кабинета Министров от 23 декабря 2020 г. №807 «О внесении дополнений в Постановление Кабинета Министров Республики Узбекистан от 5 сентября 2018 г. №707 «О мерах по совершенствованию информационной безопасности во Всемирной информационной сети Интернет»» *(Акты Кабинета Министров Республики Узбекистан от 18.02.2021 г. №12/21-04 и Министерства по развитию информационных технологий и коммуникаций Республики Узбекистан от 18.02.2021 г. №32-8/1190 и от 26.02.2021 г. №32-8/1451).* Принятие этого предложения послужило урегулированию в должном порядке отношений касательно необходимости своевременного удаления незаконной информации, размещённой во Всемирной сети Интернет, в том числе лицом разместившим информацию.

предложение об установлении в целях ограничения среди населения разного рода панической и недостоверной информации в условиях пандемии, уголовной ответственности за распространение не соответствующих действительности сведений о распространении карантинных и других опасных для человека инфекций, нашло свое отражение в статье 244^5 Уголовного кодекса Республики Узбекистан *(Акт Комитета по противодействию коррупции и судебно-правовым вопросам Законодательной палаты Олий Мажлиса Республики Узбекистан от 22.04.2021 г. № 06/1-05/1087 и Министерства по развитию информационных технологий и коммуникаций Республики Узбекистан от 18.02.2021 г. №32-8/1190 и от 26.02.2021 г. №32-8/1451).* Принятие этого предложения послужило предупреждению незаконной обработки данных о карантине в условиях пандемии;

предложения об установлении ответственности за рекламирование, демонстрацию, распространение порнографической, пропагандирующей культ насилия или жестокости продукции в сетях телекоммуникаций или Всемирной сети Интернет нашли свое отражение в статьях 130 и 130^1

Уголовного кодекса Республики Узбекистан *(Акт Комитета по противодействию коррупции и судебно-правовым вопросам Законодательной палаты Олий Мажлиса Республики Узбекистан от 22.04.2021 г. № 06/1-05/1087 и Министерства по развитию информационных технологий и коммуникаций Республики Узбекистан от 18.02.2021 г. №32-8/1190 и от 26.02.2021 г. №32-8/1451).* Принятие этого предложения послужило предупреждению распространения и незаконного использования продукции порнографического и насильственного характера.

Апробация результатов исследования. Результаты исследования были обсуждены на 11 научных конференциях, в том числе на 6 международных и 6 республиканских научных конференциях.

Опубликованность результатов исследования. По теме исследования опубликовано 22 научные работы, в том числе 1 монография, 21 научных статей (5 в зарубежных изданиях).

Структура и объём диссертации. Диссертация состоит из введения, трех глав, заключения, списка использованной литературы и приложений. Объём диссертации составляет 156 страниц.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

В введении (аннотации диссертации) обоснована актуальность темы диссертации, охарактеризованы цели и задачи, а также объект и предмет исследования, указано соответствие приоритетным направлениям науки и технологий Республики Узбекистан. Изложены научная новизна и практические результаты исследования, раскрыты теоретическая и практическая значимость полученных результатов, приведены данные о внедрении в практику результатов исследования, опубликованных работах и структуре диссертации.

Первая глава исследования посвящена ***«Теоретико-правовому анализу киберпреступлений»***, в трех параграфах данной главы анализируется понятие киберпреступлений и ее сущность, необходимость систематизации ответственности за киберпреступления в уголовном законодательстве, а также вопросы, связанные с классификацией киберпреступлений.

Первый параграф данной главы *«Понятие киберпреступления и его сущность»* посвящен раскрытию понятия киберпреступления и сущности его доктринального и официального понятий.

По мнению Диссертанта, дано определение понятию киберпреступлений напрямую связанного с развитием информационно-коммуникационных технологий, отмечается, что данное понятие с учетом развития технологий называлась «глобальная сетевая преступность», «компьютерная преступность», «преступность, связанная с компьютером», «совершение преступлений через компьютер», «электронная преступность» и «высокотехнологичная преступность», «виртуальная преступность». Кроме того, указывается, что все эти преступления совершаются в

киберпространстве, данное правило содержится в положениях Конвенции Совета Европы «О компьютерных преступлениях», являющейся международным актом и принятым 2001 года.

Во втором параграфе первой главы *«Необходимость систематизации ответственности за киберпреступления в уголовном законодательстве»,* обоснована необходимость введения уголовной ответственности за киберпреступления в уголовном законодательстве и ее систематизации.

По подсчетам руководителя Российского отдела Международной полицейской ассоциации генерал-лейтенанта Юрия Жданова, количество киберпреступлений во всем мире в 2020 году возросло на 71,4% по сравнению с 2019 годом. В результате осуществляемых государствами реформ в этой сфере, на сегодняшний день существует свыше 500 актов законодательства об охране информации, разглашении информации, компьютерной преступности, при этом, учитывая, что в Узбекистане отдельные акты законодательства, регулирующие эту сферу не разработаны должным образом, отмечается необходимость должного определения отношений касательно создания безопасного киберпространства.

В частности, в пункте 297 Государственной программы по реализации Стратегии действий по пяти приоритетным направлениям развития Республики Узбекистан на 2017-2021 годы в «Год диалога с народом и интересов человека», утвержденной Указом Президента Республики Узбекистан от 7 февраля 2017 года №УП–4947, впервые в официальном нормативно-правовом акте применяется понятие кибербезопасности и в этой сфере осуществляется ряд позитивных дел. Однако, с учетом недостаточной разработки актов законодательства в данном направлении, отсутствует возможность охватить все киберпреступления понятием «компьютерные системы или компьютерная техника», являющиеся средством или предметом преступлений, предусмотренных статьями 167-169, 278^{1}-278^{7} Уголовного кодекса, в силу своих технических возможностей. В частности, в мошенничествах, совершенных через мобильные приложения. Необходимо учесть, что мобильное приложение не является частью компьютерной системы или сети, что возрождает необходимость пересмотра национального уголовного законодательства.

В третьем параграфе этой главы *«Классификация киберпреступлений»*, из-за большого числа киберпреступлений предлагается классифицировать и изучать киберпреступления, путем подразделения их на отдельные группы. Для указания верности этого предложения, проанализированы мнения ученых компаний Tadviser, IT Skills, Kaspersky, Управления ООН по наркотическим средствам и преступности и модульного университета Серия, Евразийской группы по борьбе с отмыванием денег и финансированием терроризма, а также ученых Э.Л.Кочкиной, П.С.Титова, Наре Смбатян, Н.Лимож, М. Косович, Д.В.Пашнева, Е.Шевченко, Ю.Газизова, Т.Л.Тропиной. Изучены нормы касательно классификации киберпреступлений Закона Республики Филиппин «О предупреждении киберпреступлений» №10175, принятого в 2012 году (RA10175) пересмотренного в соответствии с ним Уголовного кодекса Филиппин,

согласно которому если любое деяние совершается посредством информационно-коммуникационных технологий, оно будет считаться киберпреступлением, и лицам, совершившим данные преступления, будет применяться наказание уровнем выше на одну ступень, по сравнению с санкцией, предусмотренной в Уголовным кодексе Филиппин[1], исследована Будапештская конвенция «О компьютерных преступлениях», предложено изучение киберпреступлений путем подразделения на следующие группы:

В частности, по способу осуществления киберпреступления делятся на две основные группы, то есть киберпреступления, совершаемые путем использования кибертехнологий, и киберпреступления, направленные против кибертехнологий. Если разъяснить это более подробнее, киберпреступления подразделяются на киберпреступления, совершаемые с использованием информационно-коммуникационных технологий и преступления, совершаемые против информационно-коммуникационных технологий. Общественно опасные деяния, предусмотренные в пункте «г» части второй статьи 103, пункте «в» части второй статьи 103^1, пункте «г» части третьей статьи 167, пункте «в» части второй статьи 168, пункте «б» части второй статьи 169, статьях 188^1, 244^1, 244^5 и 278 УК, признаются киберпреступлениями, совершенными с использованием информационно-коммуникационных технологий, а общественно опасные деяния, предусмотренные в статьях 278^1-278^7 УК, признаются киберпреступлениями против информационно-коммуникационных технологий.

В зависимости от того, в каком месте совершено общественно опасное деяние, киберпреступления можно подразделить на две группы, а именно киберпреступления, совершаемые в киберпространстве, относящимся к сфере информационно-коммуникационных технологий, и киберпреступления, совершаемые в сфере информации. Оба вида преступлений совершаются в киберпространстве, но киберпреступлениями в сфере информационно-коммуникационных технологий может быть причинен ущерб информационно-коммуникационным технологиям либо они подвержены опасности нанесения ущерба. При киберпреступлениях в сфере информации вреда информационно-коммуникационным технологиям не наносится, однако причиняется ущерб интересам лиц, общества и государства посредством хранения, передачи и использования через информационно-коммуникационные технологии информации, наносящей вред пользователям;

В зависимости от объекта совершения, киберпреступления подразделяется на киберпреступления против жизни, здоровья, нравственности, прав и интересов личности, в социально-политической, экономической сфере, против информационно-коммуникационных технологий.

---

[1] Акт, определяющий киберпреступность, обеспечивающий предупреждение, расследование, преследование и назначение наказаний за это и другие цели. Республиканский закон № 10175. 12 сентября 2012 г. https://www.officialgazette.gov.ph/2012/09/12/republic-act-no-10175/.

Вторая глава исследования озаглавлена ***«Юридический анализ киберпреступлений»***, в ней освещен юридический анализ киберпреступлений против жизни, здоровья, нравственности, прав и интересов личности, социально-политических киберпреступлений, киберпреступлений в экономической сфере, киберпреступлений против информационно-коммуникационных технологий, классифицированных по объекту совершения киберпреступлений.

В первом параграфе данной главы, посвященном *«Юридическому анализу киберпреступлений против жизни, здоровья, нравственности, прав и интересов личности»* исследованы уголовно-правовые аспекты киберпреступлений в виде доведения до самоубийства через кибертехнологии, склонения к самоубийству – киберсуицида, киберугроз, вовлечения несовершеннолетнего к антисоциальному поведению через кибертехнологии, киберпорнографии, кибернасилия, киберпритонов, киберклеветы, кибероскорбления, нарушения конфиденциальности личной жизни через кибертехнологии, нарушение законодательства о персональных данных, нарушения тайны переписки, телефонных переговоров, телеграфных или иных сообщений, нарушение авторских или изобретательских прав в отношении информационно-коммуникационных технологий, дается их юридическая характеристика.

Диссертантом проведен юридический анализ каждого вида указанных преступлений в сопоставлении с нормами международного права, уголовным законодательством зарубежных стран, исходя из осуществляемых в нашей стране реформ, а также научно обосновано в качестве эффективного решения существующих проблем предложение введения уголовной ответственности за данные преступления.

Во втором параграфе данной главы *«Уголовно-правовой анализ социально-политических киберпреступлений»*, раскрыта юридическая характеристика таких киберпреступлений, как пропаганда войны с помощью кибертехнологий, киберагрессия, кибертерроризм, киберэкстремизм, киберпосягательство против главы государства или иного должностного лица, посягательство против конституционного строя государства посредством кибертехнологий, кибершпионаж, кибердиверсия, разглашение государственной тайны через кибертехнологии, кибервзяточничество, подделка электронных документов, киберхулиганство, киберазартные игры.

Исследователем также проведен юридический анализ каждого вида указанных преступлений в сопоставлении с нормами международного права, уголовным законодательством зарубежных стран, исходя из осуществляемых в нашей стране реформ, а также научно обосновано в качестве эффективного решения существующих проблем предложено введения уголовной ответственности за данные преступления.

В третьем параграфе данной главы *«Уголовно-правовая характеристика киберпреступлений в сфере экономики»* рассмотрена юридическая характеристика киберпреступлений в виде кибервымогательства, киберрастраты, кибермошенничества, киберкражи, фальшивой киберфармацевтики, незаконной деятельности по привлечению денежных

средств и (или) другого имущества с использованием кибертехнологий. При этом обосновано, что преступления кибервымогательства, киберрастраты, кибермошенничества, киберкражи, фальшивой киберфармацевтики, незаконной деятельности по привлечению денежных средств и (или) другого имущества с использованием кибертехнологий, совершаются вменяемым лицом, достигшим 16 лет. Все эти преступления осуществляются с прямым умыслом. Вместе с тем, анализируется объект и объективная сторона этих преступлений, кроме того, юридическая характеристика данных преступлений представлена в виде отдельной таблицы в диссертации.

В четвертом параграфе *«Юридический анализ киберпреступлений против информационно-коммуникационных технологий»*, представлен юридический анализ преступлений в сфере информационных технологий регламентированных в главе XX[1] Уголовного кодекса Республики Узбекистан, в частности, нарушения правил информатизации статьи 278[1], изготовления с целью сбыта либо сбыт и распространение специальных средств для получения незаконного (несанкционированного) доступа к компьютерной системе, а также к сетям телекоммуникаций статьи 278[3], модификации компьютерной информации статьи 278[4], компьютерного саботажа статьи 278[5], создания, использования или распространения вредоносных программ статьи 278[6], незаконного (несанкционированного) доступа к сети телекоммуникаций статьи 278[7] УК. Вместе с тем, обоснована необходимость либерализации ответственности, декриминализации некоторых преступлений и их отнесения к административным правонарушениям.

При этом, диссертантом обосновано, что преступления в виде нарушения правил информатизации, незаконного доступа к компьютерной информации, изготовления с целью сбыта либо сбыта и распространения специальных средств для получения незаконного (несанкционированного) доступа к компьютерной системе, а также к сетям телекоммуникаций статьи, модификации компьютерной информации, компьютерного саботажа, создания, использования или распространения вредоносных программ, незаконного (несанкционированного) доступа к сети телекоммуникаций совершается вменяемым лицом, достигшим 16 лет. Из этих преступлений нарушение правил информатизации, незаконный доступ к компьютерной информации, модификация компьютерной информации, совершаются по неосторожности (самонадеянность или небрежность) и умышленно (прямой и косвенный умысел), изготовление с целью сбыта либо сбыт и распространение специальных средств для получения незаконного (несанкционированного) доступа к компьютерной системе, а также к сетям телекоммуникаций, компьютерный саботаж, создание, использование или распространение вредоносных программ, незаконный (несанкционированный) доступ к сети телекоммуникаций, совершаются с прямым умыслом и разработаны соответствующие предложения и рекомендации.

Третья глава исследования ***«Перспективы совершенствования назначения наказания за киберпреступления и профилактики***

киберпреступлений» посвящена рассмотрению вопросов ответственности и назначения наказания за киберпреступления, борьбы с киберпреступностью, обеспечению кибербезопасности, экспертизе совершенных киберпреступлений, определению уполномоченных органов по расследованию киберпреступлений и борьбе с киберпреступностью, а также перспективам обеспечения кибербезопасности в нашей стране.

В первом параграфе данной главы *«Особенности назначения наказания за киберпреступления»* рассмотрены особенности назначения наказания за классифицированные и входящие в эту класссификацию основные киберпреступления, правовые и технические решения по устранению ущерба, причиненного в результате совершения киберпреступления. Вместе с тем, научно обоснован порядок разрешения существующих проблем по определению действия киберпреступлений во времени и в пространстве, а также определения реально причиненного ущерба при назначении наказания. Кроме того, изучен механизм назначения наказания за киберпреступления в уголовном законодательстве таких государств, как Азербайджан, Болгария, Грузия и Филиппины.

В результате на основе предложений автора, были пересмотрены, внесены изменения и дополнения в статьи 130-130^{1}, 139-140, 141^{1}-141^{2}, 158, 244, 244^{1}, 244^{5}-244^{6} Уголовного кодекса Республики Узбекистан, была определена ответственность за совершение ряда общественно опасных деяний посредством Интернета и средства телекоммуникаций, была усилена существующая ответственность.

По мнению исследователя, объект киберпреступлений составляют общественные отношения, охраняемые посредством информационных технологий и коммуникаций, и характер посягательства на данные общественные отношения демонстрирует объективную сторону киберпреступлений. Поскольку виды и формы киберпреступлений различны, трудно четко определить ее объективную сторону, и для каждого вида киберпреступления объективная сторона выражается различным образом в зависимости от формы совершения преступления.

Во втором параграфе *«Перспективы совершенствования профилактики киберпреступлений»*, перечислены задачи, стоящие перед нашей страной в области предупреждения, противодействия и профилактики киберпреступлений, разработан механизм их реализации. Также с точки зрения международного и зарубежного опыта обосновано четкое определение полномочий государственных органов по реализации задач, поставленных в данном направлении.

Как отмечает исследователь, по мнению международных экспертов Cybersecurity Ventures, во всем мире каждые 14 секунд совершается одна кибератака, при этом по прогнозам Всемирного экономического форума, в 2022 году в результате кибератак миру будет причинен ущерб в размере 8 трлн. долларов. Ученые пытаются дать различные пояснения в части предупреждения киберпреступлений для устранения этого ущерба, так, ученые В.С. Харламов, Я. Попыева, М.А. Ефремова полагают, что

единственным решением этой проблемы является включение понятия киберпреступности в уголовный закон страны.

Диссертантом, исходя из наличия в статьях 319[a]-319f Уголовного кодекса Болгарии, статьях 284-286 Уголовного кодекса Грузии, 1-пояснительной части главы 24 Уголовного кодекса Беларуси, статье 279-а Уголовного кодекса Дании, статье 263а Уголовного кодекса Франции, статье 268 Уголовного кодекса Эстонии норм о компьютерном мошенничестве, в статье 640-ter Уголовного кодекса Италии, статье 287 Уголовного кодекса Китайской Народной Республики, абзаце третьем пункта «а» статьи 138ab Уголовного кодекса Нидерландов, статье 287 Уголовного кодекса Польши, части 3 статьи 190 Уголовного кодекса Украины, статье 247[2] Уголовного кодекса Южной Кореи, статье 478 Уголовного кодекса Испании, пункте 1 статьи 4 главы 30 Уголовного кодекса Финляндии, статье 143 Уголовного кодекса Швейцарии, статье 148а Уголовного кодекса Австрии норм определяющих ответственность за киберпреступления, даны предложения по совершенствованию Уголовного кодекса Республики Узбекистан.

Самым эффективным способом обеспечения кибербезопасности в стране является принятие стратегии кибербезопасности. Зарубежными странами – Украина, США, Эстония, Литва, Испания, Германия, Словакия, Япония, Швейцария, Норвегия, Новая Зеландия, Индия, Австралия, ЮАР, Канада, Финляндия, Австрия, Румыния, Польша, Франция, Чешская Республика, Нидерланды и Люксембург были приняты и реализуются такие стратегии. Исходя из этого, обосновано, что в пункте 243 Государственной программы по реализации Стратегии действий по пяти приоритетным направлениям развития Республики Узбекистан в 2017-2021 годах в «Год развития науки, просвещения и цифровой экономики», утвержденной Указом Президента Республики Узбекистан от 2 марта 2020 года №УП–5953 определена разработка национальной стратегии кибербезопасности, рассчитанной на 2020-2023 годы, в качестве ее реализация следует как можно скорее принять стратегию кибербезопасности.

Самой большой угрозой в обеспечении кибербезопасности является халатность государственных органов и ведомств. Следует признать, что большинство министерств и ведомств, предприятий абсолютно далеки от цифровых технологий. Обосновано, что для устранения халатности в обеспечении кибербезопасности, следует разработать необходимые государственные программы и дорожные карты и добиться воплощения их в жизнь.

З А К Л Ю Ч Е Н И Е

Разработаны следующие научно-практические предложения и рекомендации по комплексному изучению уголовно-правовых аспектов киберпреступлений:

I. Научно-теоретические выводы по развитию науки уголовного права:

1. Разработаны следующие авторские определения понятий киберпреступление, киберпреступность и кибертехнологии:

киберпреступление – это виновное, уголовно наказуемое и запрещенное Уголовным кодексом общественно опасное деяние (действие или бездействие), совершаемое в киберпространстве с использованием информационно-коммуникационных технологий либо в отношении них;

кибертехнологии – совокупность информационно-коммуникационных технологий, цифровых технологий, кибертехнологий, робототехники, программных продуктов, программно-аппаратных продуктов, телекоммуникационных средств, объектов связи, компьютерных систем, телекоммуникаций, Интернет, связи и иных сетей, систем, информационных ресурсов, информационных систем, баз данных и иных технологий.

2. В настоящее время существует более 200 видов киберпреступлений, целесообразно их изучение путем классификации. Киберпреступления можно изучить, подразделяя их на следующие группы:

по способу осуществления киберпреступления делятся на две основные группы, то есть киберпреступления, совершаемые путем использования кибертехнологий, и киберпреступления, направленные против кибертехнологий. Если разъяснить это более понятно, киберпреступления подразделяются на киберпреступления, совершаемые с использованием информационно-коммуникационных технологий и преступления, совершаемые против информационно-коммуникационных технологий. Общественно опасные деяния, предусмотренные в пункте «г» части второй статьи 103, пункте «в» части второй статьи 103^{1}, пункте «г» части третьей статьи 167, пункте «в» части второй статьи 168, пункте «б» части второй статьи 169, статьях 188^{1}, 244^{1}, 244^{5} и 278 УК, признаются киберпреступлениями, совершенными с использованием информационно-коммуникационных технологий, а общественно опасные деяния, предусмотренные в статьях 278^{1}-278^{7} УК, признаются киберпреступлениями против информационно-коммуникационных технологий;

в зависимости от того, в каком месте совершено общественно опасное деяние, киберпреступления можно подразделить на две группы, а именно киберпреступления, совершаемые в киберпространстве, относящемся к сфере информационно-коммуникационных технологий, и киберпреступления, совершаемые в сфере информации. Оба преступления совершаются в киберпространстве, но в киберпреступлениях в сфере информационно-коммуникационных технологий может быть причинен ущерб информационно-коммуникационным технологиям либо они приведены в состояние ущерба. В киберпреступлениях в сфере информации вреда

информационно-коммуникационным технологиям не наносится, однако причиняется ущерб интересам лица, общества и государства посредством хранения, передачи и использования через информационно-коммуникационные технологии информации, наносящей вред пользователям;

в зависимости от объекта совершения, киберпреступления разделяется на киберпреступления против жизни, здоровья, нравственности, прав и интересов личности, в социально-политической, экономической сфере, против информационно-коммуникационных технологий.

Все киберпреступления совершаются в киберпространстве.

II. Предложения, направленные на совершенствование уголовного законодательства Республики Узбекистан

1.

1. В соответствии с требованиями Закона Республики Узбекистан «О нормативно-правовых актах», предлагается в главу VIII Уголовного кодекса Республики Узбекистан внести сущность понятий информационно-коммуникационных технологий, цифровых технологий, кибертехнологий, киберпреступления, киберпреступности, киберправонарушения, кибербезопасности, киберпреступлений, совершаемых посредством кибертехнологий либо против них, а также внести коррективы в статьи 103, 103^{1}, 112, 127, 130-131, 139-140, 141^{1}-141^{2}, 149-150, 155^{1}, 156, 158-159, 162, 167, 167^{1}, 169, 186^{3}, 188^{1}, 228, 278, 278^{1}-278^{7}-УК РУ и дополнить статьями 143^{3}, 151^{1}, 160^{1}, 161^{1}, 165^{1}, 244а, 168^{1}, 169^{1}, 277^{1} в редакции и виде, изложенном в приложении №1 исследования. В частности, на основе предложений автора пересмотрен Уголовный кодекс Республики Узбекистан, статьи 130-130^{1}-, 139-140-, 150-, 244-244^{1}, 244^{5}-244^{6} УК были пересмотрены, установлена ответственность за рекламирование, демонстрацию, распространение порнографической продукции, продукции, пропагандирующей культ насилия или жестокости в сетях телекоммуникаций или всемирной информационной сети Интернет, оскорбление или клевета в сетях телекоммуникаций или всемирной информационной сети Интернет, публичное оскорбление или клевета в отношении Президента Республики Узбекистан с использованием сетей телекоммуникаций или всемирной информационной сети Интернет, публичные призывы к массовым беспорядкам и насилию над гражданами с использованием сетей телекоммуникаций, всемирной информационной сети Интернет, распространение материалов, содержащих угрозу общественной безопасности и общественному порядку, не соответствующих действительности сведений о распространении карантинных и других опасных для человека инфекций в условиях возникновения и распространения карантинных и других опасных для человека инфекций, ложной информации, унижающей честь и достоинство человека;

2. Предлагается принять закон Республики Узбекистан «О кибербезопасности», его проект разработан и представлен в Приложении №2 к диссертации;

3. Предлагается принять законы Республики Узбекистан «О киберагрессии», а также «О борьбе с киберпреступлениями» (разработана структура закона).

III. Рекомендации, направленные на повышение эффективности судебной практики и системы противодействия преступности:

1. В целях систематизации работ по обеспечению кибербезопасности, организации профилактика киберпреступлений разработка на основе законов Республики Узбекистан «О кибербезопасности», «О противодействии киберпреступности», «О киберагрессии» необходимых мер по обеспечению их исполнения;

2. Для обеспечения кибербезопасности на должном уровне следует принять следующие меры:

1) до сих пор не разработан единый нормативно-правовой акт о порядке защиты информационных ресурсов и информационных систем, между тем еще в 2003 году в нашем законодательстве было указано, что правовой режим информационных ресурсов и информационных систем определяется нормами, устанавливающими данное положение. Поэтому разработка единого акта, отражающего правовой режим информационных ресурсов и информационных систем, регламентация в данном акте единого определения таких понятий, как информационные ресурсы и информационные системы, правовой статус защищенной системы, информационно-коммуникационные технологии, системы, сети, защита, определение механизма их применения, единого реестра технологий, включенных в сети и системы информационно-коммуникационных технологий;

2) в соответствии с поручением Министерства по развитию информационных технологий и коммуникаций организация практики рассылки через операторов и провайдеров связи бесплатных, не облагаемых налогом смс-уведомлений, и принять меры по ознакомлению всех слоев населения с отраслевым законодательством, своевременному и должному предупреждению о киберугрозах;

3) принять меры по поэтапному обучению сферы информационно-коммуникационных технологий путем налаживания режима семья-дошкольное образование-школа-колледж-лицей-вуз-работа-семья;

4) указание при формировании государственного бюджета затрат, направленных на обеспечение кибербезопасности в отдельной смете;

5) развитие системной работы по обучению, подготовке кадров и повышению квалификации в сфере информационно-коммуникационных технологий;

6) принятие мер по обучению таких учебных программ и предметов, как право информационно-коммуникационных технологий, право

киберпреступности, основы обеспечения кибербезопасности в разрезе дошкольное образование-школа-колледж-лицей-вуз;

7) разработка и принятие методики выявления, расчета и взыскания ущерба, причиненного вследствие совершения киберпреступлений и киберправонарушений;

8) в целях всеобщего сотрудничества с международными организациями и зарубежными странами, рассмотрение возможности частичного членства в Будапештской конвенции 2001 года, а затем разработки единого международного акта по борьбе с киберпреступностью и киберправонарушениями, обеспечивающего кибербезопасность в государствах, принятия его всеми государствами с последующим выходом из Будапештской конвенции;

9) налаживание системы единой подготовки правовед-технических кадров в сфере информационно-коммуникационных технологий посредством предоставления в сфере образования как юридических, так и технических знаний касательно киберпреступности, киберправонарушений и кибербезопасности;

10) создание и практическая реализация возможности предоставления информации о кибератаках на частную собственность населения через телефон, компьютер и иные технологии, являющиеся их частной собственностью;

11) создание и внедрение в практику системы, предоставляющей возможности освобождения киберпреступников и лиц, совершивших киберправонарушения, обладающих специальными знаниями по обеспечению кибербезопасности государства, от применяемого в отношении них наказания путем службы в интересах государства, но с возмещением причиненного ущерба;

12) в целях совершенствования уголовно-процессуального законодательства, обеспечения допустимости доказательств и проведения следственных действий должным образом, принятие Постановления Пленума Верховного суда Республики Узбекистан о даче разъяснения касательно расследования преступлений, совершенных с использованием информационно-коммуникационных технологий и кибертехнологий или против них;

13) дальнейшее расширение рамок научно-исследовательских работ, направленных на решение существующих проблем в сфере обеспечения кибербезопасности и налаживание их регулярного осуществления.

SCIENTIFIC COUNCIL AWARDING OF THE SCIENTIFIC DEGREES DSc. 32/30. 12. 2020. Yu. 74. 01 UNDER THE UNIVERSITY OF PUBLIC SECURITY OF THE REPUBLIC OF UZBEKISTAN

UNIVERSITY OF PUBLIC SECURITY OF THE REPUBLIC OF UZBEKISTAN

ANORBOEV AMIRIDDIN ULUGBEK UGLI

CRIMINAL LEGAL ASPECTS OF CYBERCRIME

12.00.08 – Criminal law. Criminology. Criminal-enforcement law

ABSTRACT
of the dissertation of the Doctor of Philosophy (PhD) on science in law

Tashkent – 2021

The theme of the dissertation (PhD) was registered in the Suprime Attestation Commission under the Cabinet of Ministers of the Republic of Uzbekistan with number B2019.1.PhD/Yu274

The dissertation is prepared at the University of Public Security of the Republic of Uzbekistan.

The abstract of the dissertation is posted in three languages (Uzbek, English, Russian (summary)) onthe website of the University of Public Safety of the Republic of Uzbekistan (www.mgjxu.uz) and Information educationalportal «ZiyoNET» (www.ziyonet.uz).

Scientific supervisor:	**Rustambayev Mirzayusup Khakimovich** Doctor of Law, professor
Official opponents:	**Inagamdjanova Zumratxon Fatkhullaevna** Doctor of Law, professor
	Rasulev Abdulaziz Karimovich Doctor of Law, associate professor
Leading organization:	**Academy of the General Prosecutor's Office of the Republic of Uzbekistan**

The defense of the dissertation will take place on “27” november 2021 year at 10-00 the meeting of the Scientific Council DSc.32/30. 12. 2020. Yu. 74. 01 at the University of Public Security of the Republic of Uzbekistan. (Address: 100109, Tashkent region, Zangiota district, Chorsu kurgan. Tel.: (99871) 230-32-71; fax: (99871) 230-32-50; mgjxu@umail.uz).

The doctoral dissertation can be reviwed an the Information Resource Center of the University of Public Security of the Republic of Uzbekistan (registered as no.2166/1). (Address: 100109, Tashkent region, Zangiota district, Chorsu kurgan. Tel.: (99871) 230-32-71; fax: (99871) 230-32-50).

The abstract of the dissertation was distributed on “12” november 2021 year.

(Registry protocol № 9 dated on “12” november 2021 year).

D.M.Mirazov
Deputy Chairman of the Scientific Council for awarding Academic Degrees, Doctor of Law, Professor

M.M.Nurmatov
Secretary of the Scientific Council for Awarding Academic Degrees, Doctor of Law, Associate Professor

M.B.Usmonov
Chairman of the Scientific seminar at the Scientific Council for Awarding Academic Degrees, Doctor of Law, Professor

INTRODUCTION (abstract of doctoral thesis)

The purpose of the study is to analyze the criminal and legal aspects of cybercrime, develop scientific and practical proposals and recommendations for ensuring cybersecurity.

The object of the research work is social relations related to the legal regulation of criminal and legal aspects of cybercrime in the Republic of Uzbekistan.

The scientific novelty of the research includes following:

based on the introduction of a system of mandatory expertise of government agencies and organizations on the compliance of software, databases, including operating systems with the requirements of information and cyber security;

If the text of comments left by users of the website, as well as on social networks or messengers reveals information restricted by the Ministry of Information Technology and Communications of the Republic of Uzbekistan, the Center for Mass Communications of the Agency for Information and Mass Communications and (or) the owner of the messenger page, as well as the blogger is notified of the removal of information prohibited by the legislation of the Republic of Uzbekistan.

to publish inaccurate information about the spread of quarantine and other infectious diseases dangerous to humans in the context of the emergence and spread of quarantine and other dangerous human diseases, or to establish criminal liability for dissemination in otherwise reproduced text or media, as well as the Internet justified;

distribution, advertising, preparation or importation of pornographic, violent or cruel propaganda products into the territory of the Republic of Uzbekistan, as well as advertising, display, distribution of pornographic products, including advertising in mass media, telecommunication networks or Internet world information network based on the definition of criminal liability for making, demonstration, distribution.

Implementation of the research results. Based on the results of a study on the criminal law aspects of cybercrime:

Proposal on the introduction of a system of mandatory expertise of information systems of all government agencies and organizations in the country on compliance with information and cyber security requirements on the implementation of the Strategy "Digital Uzbekistan - 2030" for 2020-2022 Item 28 of the Roadmap (Ministry of Information Technologies and Communications Development No. 32-8 / 4040 of 16.07.2020, No. 32-8 / 1190 of 18.02.2021 and 32-8/26.02.2021 Act No. 1451). The introduction of this proposal served to ensure their cyber security through the mandatory examination of information systems of government agencies and organizations;

Proposal on the need to establish a procedure for sending a notice to the owner of the website, website and (or) messenger page, as well as the blogger on the removal of information prohibited by the legislation of the Republic of Uzbekistan on "Amendments to the Resolution No. 707 of September 5, 2018" is

reflected in paragraph 2 and the Annex to the Resolution No. 807 of December 23, 2020. (Act of the Cabinet of Ministers No. 12/ 21-04 of 18.02.2021 and the Ministry of Information Technologies and Communications Development No. 32-8 / 1190 of 18.02.2021 and No. 32-8 / 1451 of 26.02.2021).

The proposal to establish criminal liability for disseminating untrue information about the spread of quarantine and other infectious diseases dangerous to humans in order to limit various panic and inaccurate information among the population in the context of a pandemic is reflected in Article 2445 of the Criminal Code of the Republic of Uzbekistan. Committee on Combating Corruption and Judicial Issues of the Legislative Chamber of the Oliy Majlis No. 06 / 1-05 / 1087 of 22.04.2021 and the Ministry of Information Technologies and Communications No. 32-8 / 4040 of 16.07.2020, No. 32 of 18.02.2021 -8 / 1190 and Act No. 32-8 / 1451 of 26.02.2021).The introduction of this proposal served to prevent the illegal processing of quarantine data in pandemic conditions;

Proposals to establish liability for advertising, display, distribution of pornographic and violent or cruelty products on telecommunication networks or the Internet are reflected in Articles 130 and 1301 of the Criminal Code of the Republic of Uzbekistan (Legislative Chamber of the Oliy Majlis of the Republic of Uzbekistan Anti-Corruption and Judiciary) - Committee on Legal Affairs No. 06 / 1-05 / 1087 dated 22.04.2021 and the Ministry of Information Technologies and Communications Development No. 32-8 / 4040 dated 16.07.2020, No. 32-8 / 1190 dated 18.02.2021 and 26.02. Act No. 32-8 / 1451 of 2021). The introduction of this proposal served to prevent the distribution and illegal use of pornographic and violent products.

The structure and scope of the research. The content of the dissertation consists of an introduction, three chapters, a conclusion, a list of references and appendices. The volume of the dissertation is 156 pages.

ЭЪЛОН ҚИЛИНГАН ИШЛАР РЎЙХАТИ
СПИСОК ОПУБЛИКОВАННЫХ РАБОТ
LIST OF PUBLISHED WORKS

I бўлим (I часть; I part)

1. Анорбоев А.У. Кибержиноятчилик, унга қарши курашиш муаммолари ва киберхавфсизликни таъминлаш истиқболлари. Монография. – Тошкент. «IMPRESS MEDIA», 2020. – Б. 318.
2. Анорбоев А.У. Болаларнинг соғлиғига зарар етказувчи киберхавфнинг олдини олиш масалалари. – Т.: «Bola va zamon» 3/2019, –Б. 70 ISSN 2181-5496. (12.00.00 №1).
3. Анорбоев А.У. Кибертерроризм и перспективы борьбы с ним. – Т.: «Одил судлов» журнали. №9/2019. ISSN 2181-8991. – Б. 80. (12.00.00 №3).
4. Анорбоев А.У. Электрон рақамли имзо ва электрон ҳужжатларни қалбакилаштириш жинояти. – Т.: «Одил судлов» журнали. №11/2019. ISSN 2181-8991. – Б. 120. (12.00.00 №3).
5. Анорбоев А.У. Киберҳужум орқали ўзгалар мулкини талон-тарож қилиш билан боғлиқ жиноятларнинг ҳуқуқий ҳолати. – Т.: (2018) Ҳуқуқий тадқиқотлар /Правовые исследования/Journal of Law Research. 2019 (9) сон. http://dx.doi.org/10.26739/2181-9130-2019-9-7. (12.00.00 №19).
6. Анорбоев А.У. Кибермаконни яратиш бўйича ваколатли орган: мулоҳаза ва таклифлар. – Т.: «Bola va zamon» журнали. 1/2020, – Б.68. ISSN 2181-5496. (12.00.00 №1).
7. Анорбоев А.У. Кибержиноятлар хавфини бартараф этиш йўллари. – Т.: «Одил судлов» журнали. № 5/2020. ISSN 2181-8991. – 80 б. (12.00.00 №3).
8. Анорбоев А.У. Электрон ҳужжатларни қалбакилаштириш жинояти. «Huquq va burch» журнали, №11/2019. – Б. 36-41. (12.00.00 №2).
9. Анорбоев А.У. Виртуал хуруж: суицид, эгри қасд ва бошқалар... – Т.: «Huquq va burch» ижтимоий-ҳуқуқий журнали, 2020 йилдаги №9/20-сон, – Б.56-59. (12.00.00 №2).
10. Анорбоев А.У. Киберфирибгарлик жинояти: жиноий-ҳуқуқий ва криминологик тавсифи. (2018) Ҳуқуқий тадқиқотлар /Правовые исследования/Journal of Law Research. 2-махсус сон. 2020, special issue 2, – P. 300-308. Doi Journal 10.26739/2181-9130. ISSN 2181-9130. №SI-2 (2020) DOI http://dx.doi.org/10.26739/2181-9130-2020-SI-2. http://dx.doi.org/10.26739/2181-9130-2020-SI-2-38. (12.00.00 №19).
11. Anorboev A.U. Cybercrime in legislation Republics of Uzbekistan. European Journal of Research volume 5 issue 5 2020 pages 20-28. ISSN 2521-3261 (Online)/ ISSN 2521-3253 (Print). DOI 10.37057/2521-3261 https://journalofresearch.info/.
12. A.U. Anorboev. Problems of cyber security in the criminal legislation of the republic of Uzbekistan. Modern views and research – 2021

International scientific and practical Conference ISBN 978-1-83853-487-5. – P. 106-108. https://doi.org/10.5281/zenodo.5656655.

13. Анорбоев А.У. Уголовно-правовые аспекты киберпреступления. Research and Publishing Center virtualconferences.press International Journal of Engineering Mathematics: Theory and Application. ISSN 1687-6156. http://iejemta.com/. DOI 10.5281/zenodo.5567890.

14. Анорбоев А.У. Электрон рақамли имзо ва электрон ҳужжатларни тайёрлаш ва фойдаланиш қоидаларини бузишнинг ҳуқуқий ҳолати. «Қонун ижодкорлигининг замонавий тенденциялари: миллий, хорижий ва халқаро тажриба» мавзусидаги республика илмий-амалий конференция материаллари тўплами. – Ўзбекистон Республикаси Адлия вазирлиги. УЎК: 340.130.53 (100) (063), КБҚ: 67.400.6 (0)я 43. Қ–57. ISBN 978-9943-56199-1. – Т.: “Адолат” ҳуқуқий ахборот маркази, 2019 й., – Б. 312.

15. Анорбоев А.У. Кибертерроризм ва унга қарши курашишнинг қонунчилик базасини такомиллаштириш йўллари. «Қонун ижодкорлигининг замонавий тенденциялари: миллий, хорижий ва халқаро тажриба» мавзусидаги республика илмий-амалий конференция материаллари тўплами. – Ўзбекистон Республикаси Адлия вазирлиги. УЎК: 340.130.53 (100) (063), КБҚ: 67.400.6 (0)я 43. Қ–57. ISBN 978-9943-56199-1. – Т.: «Адолат» ҳуқуқий ахборот маркази, 2019 й., – Б. 312.

16. Анорбоев А.У. Киберҳужум – дастурий маҳсулот муаллифларига зарар келтирувчи жиноий фаолиятдир. Ўзбекистон Республикаси Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлиги, Муҳаммад ал-Хоразмий номидаги Тошкент ахборот технологиялари университети Ўзбекистон Радиотехника, электроника ва алоқа илмий-техника жамиятининг «Иқтисодиётнинг тармоқларини инновацион ривожланишида ахборот-коммуникация технологияларининг аҳамияти» мавзусидаги Республика илмий-техник анжумани маърузалар тўплами, 5 - 6 март 2020 йил, – Б. 409-414.

II бўлим (II часть; II part)

17. Анорбоев А.У. Киберпреступления и кибертерроризм: уголовно-правовые аспекты. – Т.: Теоретико-методологические подходы к формированию системы развития предприятий, комплексов, регионов: монография / Под. общ. ред. Ф.Е. Удалова, В.В. Бондаренко, О.А.Столяровой. – Пенза: РИО ПГАУ, 2019. – 213 С. УДК 658. ББК 65.292.1. ISBN 978-5-907181-09-0.

18. Анорбоев А.У. Проблемы борьбы против кибертерроризму и перспективы обеспечения кибербезопасности. Monografia Pokonferencyjna Science, Research, Development №19, Valletta. (Republic of Malta). 30.07.2019-31.07.2019. U.D.C. 72+7+7.072+61+082. B.B.C. 94. Z 40. (30.07.2019) - Warszawa, 2019. - 114 str. ISBN: 978-83-66401-12-9. – Б.114.

19. Anorboev A.U. Cyber crime in legislation Republic of Uzbekistan. Monografia Pokonferencyjna, Science, Research, Development №26, –

Познань/Poznan. 27.02.2020- 28.02.2020. (28.02.2020) - Warszawa, 2020. – P. 260. ISBN: 978-83-66401-35-8. U.D.C. 72+7+7.072+61+082. B.B.C. 94. Z 40.

20. Анорбоев А.У. Конституция – эркин вва озод, тинч ва осойишта фаровон ҳаётимизнинг кафолати Ўзбекистон Республикаси Конституцияси қабул қилинганлигининг 26 йиллигига бағишланган илмий-амалий конференция материаллар тўплами, – Т.: 2018 й., Ўзбекистон Республикаси Миллий Гвардияси Ҳарбий-техник институти, – 250-253 б.

21. Анорбоев А.У. Конституция – мамлакатнинг киберхавфсизлигини таъминлашнимустаҳкам пойдеворидир. Конституция – эркин вва озод, тинч ва осойишта фаровон ҳаётимизнинг кафолати Ўзбекистон Республикаси Конституцияси қабул қилинганлигининг 26 йиллигига бағишланган илмий-амалий конференция материаллар тўплами, – Т.: 2018 й., Ўзбекистон Республикаси Миллий Гвардияси Ҳарбий-техник институти, – 253-258 б.

22. Анорбоев А.У. Киберфирибгарлик жинояти: жиноий-ҳуқуқий ва криминологик тавсифи. Юридик фан ва ҳуқуқни қўллаш амалиётининг долзарб муаммолари. Илмий-амалий конференция материаллари. I жилд / Масъул муҳаррир ю.ф.д., проф. М.М.Мамасиддиқов. –Т.: «Lesson press». 2020 й., – Б. 442. ББК 67.404.

«Жамоат хавфсизлиги» журналининг таҳририятида таҳрирдан ўтказилди

Босишга рухсат этилди: 16.11.2021 йил.
Бичими 60x84 $^{1}/_{16}$, «Times New Roman»
гарнитурада рақамли босма усулида босилди.
Шартли босма табоғи: 3,1. Адади 100. Буюртма № 201.
Тел (99) 832 99 79; (97) 815 44 54.
Гувоҳнома reestr № 10-3279
“IMPRESS MEDIA” МЧЖ босмахонасида чоп этилган.
100031, Тошкент ш., Яккасарой тумани, Қушбеги кўчаси, 6-уй