ДОНИШГОҲИ МИЛЛИИ ТОҶИКИСТОН

Бо ҳуқуқи дастнавис

ВБД: 343 (575.3)

ДАВЛАТЗОДА КОМРОН ДАВЛАТ

МАСЪАЛАҲОИ ҲУҚУҚӢ-ҶИНОЯТӢ ВА КРИМИНОЛОГИИ МУҚОВИМАТ БО КИБЕРҶИНОЯТҲО: ПРОБЛЕМАҲОИ НАЗАРИЯВӢ ВА АМАЛӢ

АВТОРЕФЕРАТИ
диссертатсия барои дарёфти дараҷаи илмии доктори илмҳои ҳуқуқшиносӣ аз рӯйи ихтисоси 12.00.08 – Ҳуқуқи ҷиноятӣ ва криминология; ҳуқуқи иҷрои ҷазои ҷиноятӣ

ДУШАНБЕ – 2024

Диссертатсия дар кафедраи криминалистика ва фаъолияти экспертизаи судии факултети ҳуқуқшиносии Донишгоҳи миллии Тоҷикистон омода гардидааст.

Мушовири илмӣ: **Назаров Аваз Қувватович** – доктори илмҳои ҳуқуқшиносӣ, дотсент, мудири кафедраи криминалистика ва фаъолияти экспертизаи судии факултети ҳуқуқшиносии Донишгоҳи миллии Тоҷикистон.

Муқарризони расмӣ: **Абдуҳамитов Валиҷон Абдуҳалимович** – доктори илмҳои ҳуқуқшиносӣ, профессори кафедраи ҳуқуқи ҷиноятии Донишгоҳи славянии Россия-Тоҷикистон**;**

Салаев Нодирбек Сапарбаевич – доктори илмҳои ҳуқуқшиносӣ, дотсент, профессори кафедраи ҳуқуқи ҷиноятӣ, криминология ва муқовимат бо коррупсияи Донишгоҳи давлатии ҳуқуқии Тошкенти Ҷумҳурии Ӯзбекистон;

Азимзода Назир Бозор – доктори илмҳои ҳуқуқшиносӣ, профессор, мудири кафедраи муносибатҳои байналмилалӣ ва ҳуқуқи донишгоҳи байналмилалии забонҳои хориҷии Тоҷикистон ба номи Сотим Улуғзода.

Муассисаи пешбар: Муассисаи таълимии таҳсилоти олии касбии «Академияи Вазорати корҳои дохилии Ҷумҳурии Тоҷикистон» (ш. Душанбе).

Ҳимояи диссертатсия санаи «22» июни соли 2024, соати $10^{\underline{00}}$ дар ҷаласаи шурои диссертатсионии 6D.KOA-019-и назди Донишгоҳи миллии Тоҷикистон (734025, ш. Душанбе, кӯчаи Буни Ҳисорак, толори Шурои диссертатсионии факултети ҳуқуқшиносии ДМТ) баргузор мегардад.

Бо мазмуни диссертатсия дар сомонаи www.tnu.tj ва Китобхонаи марказии илмии Донишгоҳи миллии Тоҷикистон бо нишонии 734025, ш. Душанбе, хиёбони Рӯдакӣ 17, шинос шудан мумкин аст.

Автореферат «___» _____ соли 2024 тавзеъ шудааст.

Котиби илмии Шурои диссертатсионӣ,
доктори илмҳои ҳуқуқшиносӣ, профессор **Гадоев Б.С.**

МУҚАДДИМА

Мубрамии мавзуи таҳқиқот. Таъмини амнияти иттилоотӣ аз ҳамлаҳои киберӣ дар шароити ҷаҳонишавӣ мубрам арзёбӣ гардида, иттилоот ба объекти ба таври махсус ҳифзшаванда табдил ёфтааст. Аз ин лиҳоз бо мақсади ташаккули пардохтҳои ғайринақдӣ дар шароити рушди босуръати технологияҳои иттиллоотию коммуникатсионӣ, ташкилотҳои қарзии молиявии ватанӣ, технологияҳои муосири молиявии рақамӣ, аз қабили кортҳои пардохтии бонкӣ, ҳамёнҳои электронӣ, бонкдории мобилӣ, интернет-бонкинг, пардохтҳо тавассути POS – терминал ва QR-рамзро татбиқ менамоянд, ки дар ин замина ба захираҳои иттилоотӣ, шабакаҳои иттилоотӣ ва телекоммуникатсионӣ вобастагии бештар пайдо мегардад. Инчунин, системаи пешниҳоди хизматрасониҳои давлатӣ ва коммуналӣ дар шакли электронӣ таъсис дода шудаанд, ки ин омил барои баланд бардоштани мақоми байналмилалии кишвар ва ҷалби сармояи хориҷӣ шароити мусоид фароҳам меовард.

Бояд қайд намуд, ки технологияҳои иттилоотию коммуникатсионӣ ба рушди соҳаҳои гуногуни иқтисодиёт таъсири калон расонида, як ҷузъи системаҳои муосири идоракунӣ дар тамоми бахшҳои иқтисодиёт, идоракунии давлатӣ, мудофиа, амнияти давлатӣ ва ҳифзи ҳуқуқи инсон табдил меёбад.

Ба таври васеъ ҷорӣ намудани технологияҳои иттилоотию коммуникатсионӣ (минбаъд ТИК) дар тамоми соҳаҳои ҳаёти инсон, танзими ҳуқуқии истифодаи ТИК ва ҳифзи захираҳои иттилооти нақши махсус дорад. Дар ҷаҳони муосир иттилоотикунонии ҷомеа бо суръати хеле баланд идома дошта, киберҷиноятҳо, ҳамлаҳои киберӣ ба системаҳои иттилоотӣ, дастрасии ғайриқонунӣ ба захираҳои иттилоотие, ки дар хотираи компютер нигоҳ дошта мешаванд, як таҳдиди воқеӣ ба амнияти шахс, ҷомеа, давлат ва манфиатҳои қонунии онҳо ифода мегардад.

Солҳои охир шоҳиди он ҳастем, ки бо инкишофи технологияи иттилоотӣ ва рушди шабакаҳои интернетӣ, воситаҳои нави робита миёни муошираткунандагон ба амал омада истодааст. Муоширати интернетӣ шаклҳо ва таъсиррасониҳои гуногун дошта, ба тамоми қишрҳои ҷомеаи ҷаҳонӣ асаргузор аст. Интернет дар ҳаёти рӯзмарраи муосир таъсири глобалӣ дорад ва вобаста аз мақсади истифода намуданаш ба оқибатҳои барои ҷамъият хавнок оварда мерасонад. Маводҳои лозима ба таври маҷозӣ ва дар як лаҳза дастрас карда мешаванд. Мутаасифона, ҳангоми истифодаи номувофиқ, рушди технология метавонад бар зарари аъзои ҷомеа истифода бурда шавад ва боиси пайдо шудану такмил ёфтани зӯровариҳо ва таҳдидҳои мухталифи киберӣ гардад, ки на ҳама вақт дидашавандаю ошкоршавандаанд. Мушкилоти пешгиринамоиву муқовимат бо ин гуна зуҳуроти номатлуб бошад, махсусан аз табиати ноаён доштани онҳо вобаста аст.

Дар ин замина оид ба мубрам будани таҳқиқоти мазкур, Асосгузори сулҳу ваҳдати миллӣ – Пешвои миллат, Президенти Ҷумҳурии Тоҷикистон,

муҳтарам Эмомалӣ Раҳмон, дар Паёми солонаашон ба Маҷлиси олӣ «Дар бораи самтҳои асосии сиёсати дохилӣ ва хориҷии ҷумҳурӣ», ки санаи 28-уми декабри соли 2023 баргузор гардид, таъкид доштанд, ки вазъи мураккабу ташвишовари минтақа ва ҷаҳон, аз ҷумла торафт шиддат гирифтани раванди азнавтақсимкунии дунё, яроқнокшавии бошитоб, «ҷанги сард», таҳдиду хатарҳои муосир – терроризму экстремизм, киберҷиноятҳо ва дигар ҷиноятқориҳои муташаккили фаромиллӣ моро водор месозад, ки барои таъмин намудани амнияти мудофиавии кишварамон тадбирҳои иловагӣ андешем. Ҳамзамон, 28-уми декабри соли 2022 дар ҷаласаи тантанавӣ бахшида ба иди касбии кормандони мақомоти амнияти миллии Ҷумҳурии Тоҷикистон, Пешвои муаззами миллат, муҳтарам Эмомалӣ Раҳмон, бамаврид зикр намудаанд, ки «Мушкилоти ҷиноятҳои киберӣ ва терроризми киберӣ ҳамчун таҳдидҳои нав, ба таъмини амнияти байналмилалӣ таъсири манфии ҷиддӣ ворид кардаанд. Дар чунин шароит зарур аст, ки мақомоти амният бояд беш аз ҳар вақти дигар ҳушёр бошанд, раванду ҳодисаҳои минтақа ва ҷаҳонро мунтазам омӯзанд, таҳлил кунанд ва барои пешгирӣ кардани нақшаҳое, ки ба халалдор сохтани амнияти давлату ҷомеа ва ҳаёти осоиштаи мардум равона шудаанд, тадбирҳои қонунӣ, зарурӣ ва фаврӣ андешанд...»[1].

То соли 2008 дар қаламрави Ҷумҳурии Тоҷикистон ягон киберҷиноят ба қайд гирифта нашудааст. Дар соли 2008 ҳамаги ду ҷиноят ба қайд гирифта шудааст. Дар маҷмуъ аз 2009 то 2023 шумораи ҷиноятҳои содиршуда дар соҳаи амнияти киберӣ якбора афзуда, то имрӯз 116 ҷиноятро ташкил медиҳад. Масалан, сатҳи зиёдшавии киберҷиноятқорӣ нисбат ба соли 2008 метавонад ба таври зерин тасниф карда шавад: афзоиш нисбат ба соли 2008 дар соли 2009 – 50%, 2010 – 66%, 2011 – 30%, дар солҳои 2012-2013 рақамҳо чандон фарқ намекунанд (яъне дар ин солҳо 2 киберҷиноят ба қайд гирифта шудааст), 2014 – 33,3%, 2015 – 85,71%, 2016 – 75%, 2017 – 30,46%, дар солҳои 2018-2019 нишондодҳои ҷиноятқорӣ низ чандон фарқ намекунанд (яъне дар ин солҳо 13 киберҷиноят ба қайд гирифта шудааст), 52% – дар соли 2020, дар соли 2021 ягон ҷиноят ба қайд гирифта нашудааст, 42,5% – соли 2022 ва 49,05% – дар 6 моҳи соли 2023 ташкил медиҳад)[2].

Мавриди ба зикри хос аст, ки дар миёнаи асри XXI захираҳои иттилоотӣ ба сарвати миллӣ табдил ёфта, самаранокии истифодаи онҳо қудрати иқтисодии ҳар як кишварро муайян карда, ин гуна ҷиноятҳо, натанҳо ба амнияти милли ҳар як давлат, балки масъалаҳои иҷтимоӣ ва фарҳангии аҳолиро, низ таҳти хатари ҷиддӣ қарор медиҳад. Бояд тазаккур дод, ки тибқи маълумоти Форуми Ҷаҳонии Иқтисодӣ (минбаъд ФҶИ), шахсоне, ки тавассути истифодаи ТИК дар фазои маҷозӣ (дар шакли «мустақим») ҷиноят содир менамоянд, яке аз панҷ хатари асосии ҷаҳонии таҳдидкунда ба амнияти

[1] Саҳифаи расмии интернетии Президенти Ҷумҳурии Тоҷикистон [Захираи электронӣ]. – Манбаи дастрасӣ: http://www.president.tj (санаи мурочиат: 29.12.2023).

[2] Ниг.: Маълумотномаи омории расмии Сармаркази иттилоотӣ-таҳлилии ВКД ҶТ аз 25 ноябри соли 2023, таҳти №14/3-1355.

иқтисодӣ ба ҳисоб меравад, зеро дар мавҷудият ва фаъолияти муваффақонаи тамоми бахшҳои иқтисодиёт чунин шахсон хатар эҷод менамоянд. Дар асоси гузориши ФҶИ, танҳо дар соли 2019 талафоти иқтисоди ҷаҳонӣ аз ҳамлаҳои кибернӣ 2,5 триллион доллярро ташкил дода, дар соли 2022 ин рақам ба 8 триллион доллар баробар гардид[3].

Дар робита ба ин имрӯзҳо дар шабакаҳои иҷтимоӣ рекламаҳои бардурӯғ ва фиреби қаллобон зиёд ба мушоҳида расида, баъзе шаҳрвандон ба онҳо бовар карда, бо интиқоли маблағҳои калони пулӣ зарари моддӣ-иқтисодӣ дида истодаанд, ки ҳолати мазкур нигаронкунанда буда, хисороти ин навъи ҷиноятҳо ба иқтисодиёти Ҷумҳурии Тоҷикистон аз рӯйи табиати худ хеле бузург аст. Масалан як чанд ҳолати паҳн намудани эълонҳои бардурӯғ дар шабакаи интернет, ки ба онҳо шаҳрвандон бовар намудаанд ва ҳамарӯза дар шабакаҳои иҷтимоӣ дар гардиш қарор доранд ин дастгирии молиявӣ ва иштирок дар лоиҳаҳои сармоягузории ширактҳои қаллобии хориҷӣ ба монанди «Газпром-инвест, Алиф-инвест, Тесла-х», ва ғайра аз ҷумлаи онҳое ифода мегардад, ки бо роҳи фиреб барои тасарруфи маблағҳои шаҳрвандон ташкил ва роҳандозӣ мегарданд. Пешниҳоди кӯмакҳои молиявӣ аз ҷониби сиёсатмадорон ва шахсони саховатманд низ дар марбути ин масъала мебошад. Ҳолати дигар ин мерос мондани маблағ аз хешовандони дур, пешниҳод намудани туҳфаҳо аз хориҷӣ кишвар дар намуди «баста (посилка)», албатта самтҳо ва намудҳои қаллобӣ дар интернет зиёд шуда истодаанд ва вақте сару садоҳҳо оиди қаллобӣ дар интернет ва маблағҳои аздастрафта зиёд мешаванд, онҳо иловатан роҳҳои нави содир намудини ин кирдори ба ҷамъият хавфнокро ҷӯё шуда, барномаҳои навро таҳия менамоянд ва дар сомонаҳои интернетӣ ҷойгир менамоянд[4]. Танҳо аз ҳисоби қаллобӣ дар фазои маҷозӣ, ки ҳамчун намуди нави киберҷиноятҳо эътироф мегардад, дар давраи аввали соли 2023 ба шахсони воқеӣ, зиёда аз 1 миллион сомонӣ ва дигар намуди киберҷиноятҳо, аз ҷумла ғайриқонуни даромадан ба иттилооти компютерӣ ва тағйир додани иттилооти компютерӣ дар давоми 5 соли охир ба шахсони ҳуқуқӣ зиёда аз 2090377,95 сомонӣ ба миқдори махсусан калон зарари моддӣ расонида шудааст, ки дар маҷмуъ 1000750,569 сомониро ташкил медиҳад[5]. Тибқи маълумотҳои омории Сармаркази таҳлилӣ-иттилоотии Вазорати корҳои дохилии Ҷумҳурии Тоҷикистон, аввалин киберҷиноятҳо дар Ҷумҳурии Тоҷикистон, соли 2008 ба қайд гирифта шуда буд. Шуруъ аз ҳамин давра содир гардидани он дар шаклҳои гуногун аз ҷумла таввасути сомонаҳои интернетӣ, ТИК ва компютерҳо мушоҳида гардида, дар панҷ соли охир шиддатнокии содиршаваии он таввасути сомонаҳои интернетӣ ба қайд

[3]Ниг.: Лавров С.В. Глобальные проблемы кибербезопасности и международные инициативы России по борьбе с киберпреступностью / С.В. Лавров // Внешнеэкономические связи. – Октябрь 2020. – С. 6-13.

[4]Ниг.: [Захираи электронӣ]. – Манбаи дастрасӣ: https://www.facebook.com/nbt.tj/videos/12526540187 52070/?extid (санаи мурочиат: 29.12.2023).

[5]Ниг.: Маълумотномаи омории расмии Сармаркази иттилоотӣ-таҳлилии ВКД ҶТ аз 25 ноябри соли 2023, таҳти №14/3-1355; Саҳифаи расмии интернетии Прокуратураи Генералии Ҷумҳурии Тоҷикистон [Захираи электронӣ]. – Манбаи дастрасӣ: www.prokuratura.tj/ (санаи мурочиат: 01.06.2023).

гирифта шудааст. Чунончи, танҳо дар соли 2022 аз ҷониби Раёсати мубориза бар зидди ҷиноятҳои муташаккили ВКД Ҷумҳурии Тоҷикистон 17 ҳолати киберҷиноятҳо ошкор гардида, зиёда аз 500 ҳодиса бо истифода аз интернет ва ТИК ба қайд гирифта шудааст.

Солҳои охир заминаи меъёрии ҳуқуқӣ дар самти муқовимат бо киберҷиноятқорӣ дар сатҳи миллӣ, минтақавӣ ва байналмилалӣ фаъолона инкишоф меёбад. Дар баробари ин, дар микёси ҷаҳонӣ то ҳол механизми ягонаи байналмилалии ҳуқуқии муқовимат бо киберҷиноятҳо вуҷуд надошта, дар ин самт истилоҳоти ягона таҳия нашудааст, ки ин омил ҳамкории давлатҳоро дар самти мазкур мушкил месозад. Зеро омори содиршавии киберҷиноятҳо дар кишварҳои аъзои ИДМ нишон медиҳад, ки дар соли 2020 шумораи ҷиноятҳои бақайдгирифташуда, дар самти киберҷиноятҳо 4 маротиба афзудааст: яъне аз 125 244 ҳолат дар соли 2018 то ба 536 516 ҳолат дар соли 2020. Соли 2020 дар кишварҳои аъзои ИДМ, ҳиссаи парвандаҳои ҷиноятӣ бо ҳукми айбдоркунӣ ба суд ирсолшуда 18,2% (2019 – 23%, 2018 – 24,8%) аз шумораи умумии ҷиноятҳои ба қайд гирифташуда дар ин самтро ташкил медиҳад, ки 73,6% дар соли 2020 ошкор нашуда монданд (солҳои 2018 – 66,5%; 2019 – 68,4%)[6].

Ҳамин тавр, нуқтаҳои зикршуда мубрамияти масъалаи таҳқиқоти диссертатсионии мазкурро асоснок менамояд.

Дараҷаи таҳқиқи мавзуи илмӣ. Масъалаҳои ҳуқуқӣ-ҷиноятӣ ва криминологии муқовимат бо киберҷиноятҳо ҳам аз нигоҳи назария, ва амалия давоми чандин сол аст, ки диққати муҳаққиқон ва кормандони мақомоти ҳифзи ҳуқуқро ба худ ҷалб кардааст. Масъалаҳои ҳуқуқӣ-ҷиноятии муқовимат бо киберҷиноятҳо ба таври умум дар асарҳои илмии ҳуқуқшиносонӣ ватанию хориҷӣ, аз ҷумла дар корҳои илмии В.А. Абдухамитов[7], Н.Б. Азимзода ва З.А. Саидзода[8], Ю.М. Батурин[9], И.Р. Бегишев[10], С.Ю. Битко[11], С.Д. Бражник[12], Л.А. Букалерова[13], В.В. Воробев[14], К.Н. Евдо-

[6] Ниг.: Сводные отчеты «О состоянии преступности и результатах расследования преступлений» на территории государств-участников СНГ за январь-декабрь 2018 г., 2019 г., 2020 г. // Ф.785 КН.1.; Состояние преступности в государствах-участниках СНГ в 2019 году [Захираи электронӣ]. – Манбаи дастрасӣ: https://www.ksgp-cis.ru/about/obzory/sostojanie-prestupnosti-v-2019-godu (санаи мурочиат: 21.04.2023).

[7] Ниг.: Абдухамитов В.А. Борьба с религиозным экстремизмом: уголовно-правовые, криминоло-гические проблемы (на материалах Республики Таджикистан): дис. ... д-ра юрид. наук. – Душанбе, 2016. – 335 с.

[8] Ниг.: Азимзода Н.Б., Саидзода З.А. Таърих ва моҳияти иҷтимой-ҳуқуқии ҷанги иттилоотӣ / Н.Б. Азимзода, З.А. Саидзода // Осори Академияи ВКД Ҷумҳурии Тоҷикистон. – 2021. – №4 (52). – С. 84-91.

[9] Ниг.: Батурин Ю.М. Компьютерная преступность и компьютерная безопасность. – М.: Юрид. лит., 1991. – 160 с.

[10] Ниг.: Бегишев И.Р. Понятие и виды преступлений в сфере обращения цифровой информации: дис. ... канд. юрид. наук. – Казань, 2017. – 204 с.

[11] Ниг.: Бытко С.Ю. Некоторые проблемы уголовной ответственности за преступления, совершаемые с использованием компьютерных технологий: дис… канд. юрид. наук. – Саратов, 2002. – 204 с.

[12] Ниг.: Бражник С.Д. Преступления в сфере компьютерной информации: проблемы законодательной техники: дис. ... канд. юрид. наук. – Ижевск, 2002. – 189 с.

[13] Ниг.: Букалерова Л.А. Информационные преступления в сфере государственного и муниципального управления: законотворческие и правоприменительные проблемы: дис. ... д-ра юрид. наук. – М., 2007. – 574 с.

[14] Ниг.: Воробьев В.В. Преступления в сфере компьютерной информации: юридическая характеристика составов и квалификация: дис. ... канд. юрид. наук. – Н. Новгород, 2000. – 201 с.

кимов[15], У.В. Зинина[16], П.Н. Кобетс[17], В.С. Комиссаров[18], Н.А. Қудратов[19], Ю.И. Ляпунов[20], Д.Г. Малишенко[21], З.Ҷ. Маҷидзода, А.Ғ. Холиқзода ва Р.С. Одиназода[22], А.Қ. Назаров[23], Н.Ҷ. Назаров[24], С.А. Пашин[25], А.Э. Побегайло[26], Л.Н. Попов[27], М.А. Простосердов[28], Д.В. Пучков[29], Р.Ҳ. Раҳимзода[30], Ҳ.С. Сафарзода ва Ш.Т. Аҳёзода[31], О.М. Сафонов[32], Т.Г. Смирнов[33], М.В. Старичков[34], В.Г. Степанов-Егиянтс[35], А.В. Суслопаров[36], Т.Л. Тропин[37],

[15] Ниг.: Евдокимов К.Н. Противодействие компьютерной преступности: теория, законодательство, практика. дис. ... д-ра юрид. наук. –Москва, 2021. – 557 с.

[16] Ниг.: Зинина У.В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве: дис. ... канд. юрид. наук. – М., 2007. – 160 с.

[17] Ниг.: Кобец П.Н. О современных информационных технологиях, используемых экстремистскими и террористическими группировками, и необходимости противодействия киберпреступности / П.Н. Кобец // Вестник развития науки и образования. – 2016. – №6. – С. 4-9.

[18] Ниг.: Российское уголовное право. Особенная часть / Под ред. В.С. Комиссарова. – СПб.: Питер, 2008. – 720 с.

[19] Ниг.: Кудратов Н.А. Уголовно-правовая охрана основ конституционного строя и безопасности государства: проблемы доктрины, правоприменения и совершенствования законодательства: дис. ... д-ра юрид. наук. – Душанбе, 2021. – 540 с.

[20] Ниг.: Ляпунов Ю.И., Максимов В.Ю. Ответственность за компьютерные преступления / Ю.И. Ляпунов, В.Ю. Максимов // Законность. – 1997. – №1. – С. 7-12.

[21] Ниг.: Малышенко Д.Г. Уголовная ответственность за неправомерный доступ к компьютерной информации: дис. ... канд. юрид. наук. – М., 2002. – 166 с.

[22] Ниг.: Маҷидзода З.Ҷ., Холиқзода А.Ғ., Одиназода Р.С. Ҷавонон ва амнияти иттилоотӣ (дар масири ҷаҳонишавӣ). – Душанбе, 2019. – 240 с.

[23] Ниг.: Назаров А.Қ., Давлатзода К.Д. Таҳлили муқоисавии ҳуқуқии ҷиноятӣ дар самти муборизa бар зидди ҷиноятҳои компютерӣ дар кишварҳои аъзои ИДМ ва дигар давлатҳои хориҷӣ / А.Қ. Назаров, К.Д. Давлатзода // Паёми Донишгоҳи миллии Тоҷикистон. Бахши илмҳои иҷтимой-иқтисодӣ ва ҷамъиятӣ. – 2022. – №3. – С. 229-236.

[24] Ниг.: Маҷидзода Ҷ.З., Назаров Н.Ҷ. Ҷиноятҳои муташаккил ва трансмиллӣ. – Душанбе, 2014. – 268 с.

[25] Ниг.: Комментарий к Уголовному кодексу Российской Федерации / Под общ. ред. Ю.И. Скуратова, В.М. Лебедева / Авт. главы С.А. Пашин. – М.: ИНФРА-М: Норма, 2002. – 960 с.

[26] Ниг.: Побегайло А.Э. Борьба с киберпреступностью: учеб. пособие. – М., 2018. – 184 с.

[27] Ниг.: Информационное право: учебник / Л.Л. Попов, Ю.И. Мигачев, С.В. Тихомиров. – М.: Норма: ИНФРА-М, 2010. – 496 с.

[28] Ниг.: Простосердов М.А. Экономические преступления, совершаемые в киберпространстве. – М.: Юрлитинформ, 2017. – 168 с.

[29] Ниг.: Пучков Д.В. Кибертерроризм как новая угроза современного общества / Д.В. Пучков // Виктимология. – 2021. – Т. 8. – №4. – С. 382-390.

[30] Ниг.: Раҳимзода Р.Ҳ. К новым реалиям через уроки и выводы / Р.Ҳ. Раҳимзода // Сотружество. Журнал совета министров внутренних дел СНГ. – 2021. – №1. – С. 4-11.

[31] Ниг.: Сафарзода Ҳ.С., Аҳёзода Ш.Т. Вижагиҳои хосси ҷиноятҳои характери экстремистидошта, ки бо истифодаи ВАО, шабакаҳои алоқаи барқӣ, аз ҷумла Интернет, содир карда мешаванд / Ҳ.С. Сафарзода, Ш.Т. Аҳёзода // Осори Академияи ВКД Ҷумҳурии Тоҷикистон. – 2021. – №4 (52). – С. 92-100.

[32] Ниг.: Сафонов О.М. Уголовно-правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и правоприменительной практики, перспективы совершенствования: дис. ... канд. юрид. наук. – М., 2015. – 222 с.

[33] Ниг.: Смирнова Т.Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации: дис. ... канд. юрид. наук. – М., 1998. – 161 с.

[34] Ниг.: Старичков М.В. Умышленные преступления в сфере компьютерной информации: уголовно-правовая и криминологическая характеристики: автореф. дис. ... канд. юрид. наук. – Иркутск, 2006. – 29 с.

[35] Ниг.: Степанов-Егиянц В.Г. Методологическое и законодательное обеспечение безопасности компьютерной информации в Российской Федерации: уголовно-правовой аспект: дис. ... д-ра юрид. наук. – М., 2015. – 389 с.

[36] Ниг.: Суслопаров А.В. Информационные преступления: дис. ... канд. юрид. наук. – Красноярск, 2008. – 249 с.

[37] Ниг.: Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. ... канд. юрид. наук. – Владивосток, 2005. – 234 с.

Ф.Р. Шарифзода[38], Р.Ш. Шарофзода[39], В.В. Челноков[40] ва дигарон ба риштаи таҳлил кашида шудааст. Дар заминаи таҳқиқотҳои диссертатсионӣ, олимони зикр гардида тавонистаанд, паҳлуҳои гуногуни ин кирдорҳои барои ҷамъият хавфнокро, дар фазои маҷозӣ таҳқиқ намоянд.

Вобаста ба масъалаҳои криминологии киберҷиноятҳо корҳои илмии олимони соҳа А.П. Алексеев[41], С.Э. Баҳриддинов[42], А.А. Жмихов[43], В.Э. Керимов[44], Т.П. Кесареева[45], В.В. Крилов[46], В.С. Овчинского[47], А.Л. Осипенко[48], А.Э. Побегайло[49] ва дигарон бахшида шудааст. Асарҳои олимони зикр гардида имкон медиҳанд маълумотҳои (тасаввуроти) муайянро оиди моҳият ва мундариҷаи киберҷиноятҳо ташаккул дод, аммо мутаассифона, амалан ба мушкилоти замони муосир (таҳдидҳои киберӣ ба амнияти иттилоотӣ) ва қонунгузории ҷиноятии Ҷумҳурии Тоҷикистон дар ин соҳа таъсир намерасонанд.

Асарҳои онҳо, ба вазъиятии воқеии фазои иттилоотии ҷаҳон, таҷрибаи амалии кормандони воҳидҳои оперативии субъектони муборизабарнда бо киберҷиноятҳо ва хатари он ба ҷомеа бахшида шудааст, ки ин асарҳо барои рушди доктринаи ҳуқуқӣ-ҷиноятӣ дар муқовимат бо киберҷиноятҳо аҳаммияти бузург доранд, зеро дар миқёси ҷаҳонӣ то ҳол механизми ягонаи байналмилалии ҳуқуқии муқовимат бо киберҷиноятҳо вуҷуд надошта, дар ин самт истилоҳоти ягона таҳия нашудааст, ки ин омил ҳамкории давлатҳоро дар ин самт мушкил месозад.

---

[38] Ниг.: Шарифзода Ф.Р. Теоретико-правовые основы организации деятельности органов внутренних дел Республики Таджикистан в системе обеспечения национальной безопасности государства: монография / Под ред. д.ю.н., профессора, Заслуженного юриста Российской Федерации Анатолий Михайловича Кононова. – Душанбе: ЭР-граф, 2023. – 267 с.

[39] Ниг.: Шарофзода Р.Ш., Шокиров Ғ.А. Заминаҳои илмӣ-ҳуқуқии иттилоотонӣ ва бунёди ҷомеаи иттилоотӣ дар Ҷумҳурии Тоҷикистон / Р.Ш. Шарофзода, Ғ.А. Шокиров // Осори Академияи ВКД Ҷумҳурии Тоҷикистон. – 2021. – №4 (52). – С. 110-120.

[40] Ниг.: Челноков В.В. Компьютерная информация как предмет преступления в отечественном уголовном праве: дис. ... канд. юрид. наук. – Екатеринбург, 2013. – 226 с.

[41] Ниг.: Алексеева А.П. Киберпреступность: основные черты и формы проявления / А.П. Алексеева, О.Н. Ничуговская // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. – 2017. – №1. – С. 27-34.

[42] Ниг.: Баҳриддинов С.Э. Криминология: китоби дарсӣ. Қисми умумӣ. – Душанбе, 2013. – 187 с.

[43] Ниг.: Жмыхов А.А. Компьютерная преступность за рубежом и ее предупреждение: дис. ... канд. юрид. наук. – М., 2003. – 178 с.

[44] Ниг.: Керимов В.Э., Керимов В.В. Профилактика и предупреждение преступлений в сфере компьютерной информации / В.Э. Керимов, В.В. Керимов // Черные дыры в российском законодательстве. – 2002. – №1. – С. 503-513.

[45] Ниг.: Кесареева Т.П. Криминологическая характеристика и проблемы предупреждения преступности в российском сегменте сети Интернет: автореф. дис... канд. юрид. наук. – М., 2002. – 25 с.

[46] Ниг.: Крылов В.В. Криминалистические проблемы оценки преступлений в сфере компьютерной информации / В.В. Крылов // Уголовное право. – 1998. – №3. – С. 83-91.

[47] Ниг.: Овчинский В.С. Криминология цифрового мира: учебник для магистратуры. – М.: Норма: ИНФРА-М, 2018. – 352 с.

[48] Ниг.: Осипенко А.Л. Организованная преступная деятельность в киберпространстве: тенденции и противодействие / А.Л. Осипенко // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2017. – №4 (40). – С. 181-188.

[49] Ниг.: Побегайло А.Э. Киберпреступность: учеб. пособие (для бакалавров). – М., 2014. – 96 с.

Албатта, дар ин самт ҷанбаҳои омӯхтанашуда зиёданд, ки дар ин росто омӯзиши муфассали қонунгузории ҷиноятӣ ва масъалаҳои криминологии таъмини амнияти иттилоот аз ҳамлаҳои кибернӣ зарур аст. Дар шароити ҷаҳонишавӣ бояд дар бораи мафҳуми киберҷиноятҳо ва хатари он барои ҷомеа, таснифи киберҷиноятҳо, ҳамкориҳои байналмилалӣ дар мубориза бо киберҷиноятҳо андеша кард.

Робитаи таҳқиқот бо барномаҳо ва ё мавзуъҳои илмӣ. Таҳқиқоти диссертатсионӣ дар доираи «Барномаи давлатии муқовимат бо ҷиноятқорӣ дар Ҷумҳурии Тоҷикистон барои солҳои 2021-2030» ва корҳои илмӣ-таҳқиқотии назди кафедраи криминалистика ва фаъолияти экспертизаи судӣ ва кафедраи ҳуқуқи ҷиноятӣ ва муқовимат бо коррупсияи факултети ҳуқуқшиносии ДМТ, омода гардидааст.

ТАВСИФИ УМУМИИ ТАҲҚИҚОТ

Мақсади таҳқиқот. Мақсади таҳқиқоти диссертатсионӣ омӯзиши масъалаҳои ҳуқуқӣ-ҷиноятии киберҷиноятҳо, паҳлӯҳои криминологии он, таҳияи асосҳои назариявӣ ва амалии муқовимат бо киберҷиноятҳо дар Ҷумҳурии Тоҷикистон дар шароити ҷаҳонишавӣ, рушди босуръати ТИК ва таҳдиду хатарҳои ҳамлаҳои кибернӣ ба амнияти иттилоотии кишвар, ичунин пешниҳоди навгониҳо оид ба баланд бардоштани самаранокии танзими ҳуқуқӣ-ҷиноятӣ ва криминологии муқовимат бо киберҷиноятҳо ифода мегардад.

Вазифаҳои таҳқиқот. Барои ноил шудан ба ҳадафҳои мазкур ҳалли вазифаҳои зерин зарур аст:

– омӯхтан ва муайян кардани таҳаввулоти вирусҳои компютерӣ ҳамчун омили асосии ташаккули киберҷиноятҳо;

– таҳлил ва пешниҳоди мафҳуми киберҷиноятҳо;

– муайян намудани номгуи киберҷиноятҳо ва асосҳои таснифи онҳо;

– тартиби ба роҳ мондани ҳамкории байналмилалӣ дар муқовимат бо киберҷиноятҳо;

– таҳқиқ ва таҳлили ҷавобгарӣ барои киберҷиноятҳо тибқи қонунгузории ҷиноятии кишварҳои хориҷӣ ва давлатҳои пасошӯравӣ;

– омӯзиши фарқияти ҷавобгарии ҷиноятӣ барои киберҷиноятҳо тибқи қонунгузории ҷиноятии кишварҳои хориҷӣ;

– таҳлили илмӣ-амалии аломатҳои объективии ҷиноятҳо ба муқобили шабакаҳои интернетӣ ва таҷҳизотҳои ёрирасони онҳо (барномаҳои зарароварҳ, ҳамлаҳои DoS);

– баррасӣ ва муайян кардани аломатҳои субъективии ҷиноятҳо ба муқобили шабакаҳои интернетӣ ва таҷҳизотҳои ёрирасони онҳо (барномаҳои зарароварҳ, ҳамлаҳои DoS);

– омӯзиш баррасӣ ва муайян кардани аломатҳои объективии ҷиноятҳое, ки бо истифода аз воситаҳои гуногуни техникӣ содир мешаванд (мактуби фишингӣ, кибертаъқиб, дуздии онлайнии маълумоти шахсӣ);

– таҳлили таҷрибаи ҳуқуқии аломатҳои субъективии ҷиноятҳое, ки бо истифода аз воситаҳои гуногуни техникӣ содир мешаванд (мактуби фишингӣ, кибертаъқиб, дуздии онлайнии маълумоти шахсӣ);

– таҳлили ҳолат, сохтор ва пастуболоравии (динамикаи) киберҷиноятҳо;

– баррасии хусусиятҳои криминологии шахсияти киберҷинояткор;

– таҳлил, огоҳонидан ва пешгирии киберҷиноякторӣ.

Объекти таҳқиқот. Ба сифати объекти таҳқиқот маҷмуи муносибатҳои ҷамъиятие баромад менамоянд, ки бинобар сабаби содир шудани киберҷиноятҳо ба вуҷуд меоянд.

Мавзуи таҳқиқот – ин меъёрҳои қонунгузории ҷиноятии давлатҳои хориҷӣ ва Ҷумҳурии Тоҷикистон, муқаррароти дигар санадҳои меъёри ҳуқуқие, ки ба муқовимат бо киберҷиноятҳо нигаронида шудаанд, маводҳои парвандаҳои ҷиноятӣ аз бойгонӣ, ки аз ҷониби судҳои ҶТ ва ё аз ҷониби мақомоти таҳқиқию тафтишӣ баррасӣ гардидаанд, ифода меёбад.

Марҳила, макон ва давраи таҳқиқот (доираи таърихии таҳқиқот) нақшавӣ буда, макони таҳқиқот кафедраи криминалистика ва фаъолияти экспертизаи судии факултети ҳуқуқшиносии Донишгоҳи миллии Тоҷикистон мебошад. Давраи таҳқиқот солҳои 2019-2024-ро дар бар гирифта, аз ду марҳила иборат аст.

Дар марҳилаи аввал (солҳои 2019-2020) захираҳои илмию иттилоотӣ вобаста ба мавзуи таҳқиқотӣ ба низом дароварда шуда, аз ҷониби Шурои олимон тасдиқ гардид.

Дар марҳалаи дуюм (солҳои 2020-2024) ҳадафу вазифаҳои гузошташуда иҷро гардиданд. Доир ба мавзуи таҳқиқотӣ мақолаҳои илмӣ ба табъ расида диссертатсия омода карда шуд. Лоиҳаи Қонуни Ҷумҳурии Тоҷикистон «Дар бораи амнияти киберӣ» омода карда шуданд.

Маводи таҳқиқоти диссертатсионӣ ба расмият дароварда шуд. Нисбатан муфассалтар таҳқиқот ба омӯзиши даврае равона гардидааст, ки пас аз қабули Кодекси нави ҷиноятӣ солҳои 1998-2023 дар Ҷумҳурии Тоҷикистон оғоз меёбад.

Асосҳои назариявии таҳқиқот. Асосҳои назариявии таҳқиқоти диссертатсиониро Паёмҳои Президенти Ҷумҳурии Тоҷикистон, Асосгузори сулҳу вахдати миллӣ – Пешвои миллат, муҳтарам Эмомалӣ Раҳмон, маҷмуи асарҳои назариявӣ ва амалиявӣ дар самти проблемаҳои асосии доктринаи ҳуқуқии ҷиноятӣ, вобаста ба мавзуи таҳқиқшаванда ва асарҳои олимони ватанию хориҷӣ, аз ҷумлаи В.Б. Вехов, А.Г. Волеводз, Ю.В. Гаврилин, Л.Д. Галиакбаров, А.А. Гаухман, Т.А. Герсензон, В.А. Голубев, А.И. Долгов, Г.А. Есаков, А.М. Жодзишский, Р.В. Жубрин, О.С. Капинус, М.И. Ковалев, И.Я. Козаченко, В.Е. Козлов, В.С. Комиссаров, А.И. Коробеев, С.М. Кочои, В.Н. Кудрявсев, Н.Ф. Кузнетсов, Б.А. Куринов, В.Д. Курушин, А.Н. Ларков, В.Н. Лопатин, Н.А. Лопашенко, В.В. Лунеев, Ю.И. Ляпунов, З.Ҷ. Маҷидзода, А.Қ. Назаров, А.В. Наумов, Б.С. Никифоров, С.И. Никулин, В.А. Номоконов, К.В. Ображиев, В.С. Овчинский, А.Л. Осипенко, А.В. Павлинов, С.В. Пархоменко,

А.А. Пионтковский, С.В. Полубински, А.И. Рарог, Т.В. Раскина, И.М. Рассолов, С.В. Расторопов, Р.Ҳ. Раҳимзода, В.С. Савелев, А.И. Сафарзода, Д.А. Соколов, Н.С. Тагантсев, А.Н. Трайнин, А.Ғ. Холиқзода, А.И. Чучаев, Т.Ш. Шарипов, Ф.Р. Шарифзода, Р.Ш. Шарофзода, П.С. Яни аҳаммияти калони назариявӣ доранд.

Олимони мазкур барои таҳлил намудани проблемаҳои содиршавии киберҷиноятҳо, муайян намудани шахсияти киберҷинояткор (хакер) пешгирии киберҷиноятҳо ва таснифи киберҷиноятҳо дар самти ҷиноятҳо муқобили амнияти иттилоотӣ заминаи муносиби назариявӣ фароҳам овардаанд.

Илова бар ин, асоси назариявии таҳқиқотро нашрияҳои илмии захираҳои электронии интернетӣ, ки ба масъалаҳои ҳуқуқӣ-ҷиноятӣ ва криминологии муқовимат бо киберҷиноятҳо бахшида шудаанд, ташкил медиҳанд.

Асосҳои методологии таҳқиқот. Дар ҷараёни таҳқиқот методҳои диалектикӣ, ичунин барои ҳалли вазифаҳои гузошташуда бо истифода аз равишҳо ва усулҳои институтсионалӣ, расмӣ-ҳуқуқӣ, расмӣ-мантиқӣ, муқоисави-ҳуқуқӣ, оморӣ ва дигар методҳои умумӣ ва махсуси илмӣ, ки ҷониби илм таҳия ва дар амалия санҷидашудаанд, истифода шуданд. Методҳои умумӣ-илмӣ имкон дод, ки омӯзиши нақши технологияҳои иттилоотӣ-коммуникатсионӣ, дар рушди ҷомеа ва таъсири онҳо ба ҷомеаи муосир, истифодаи бемавриди онҳо дар шароити ҷаҳонишавӣ чӣ паёмадҳо дорад. Методологияи дар таҳқиқ истифодашуда шароит фароҳам овард, ки он ҳамаҷониба анҷом ёфта, пайдоиши падидаҳо ва зерпадидаҳои нав муайян карда шавад, инчунин тамоюлҳои нави ҳамкориҳои байналмилалӣ дар муқовимат бо киберҷиноятҳо муайян карда шаванд ва идеяҳои нав ҷиҳати самаранок амалӣ сохтани онҳо дар таҷриба пешниҳод карда шаванд.

Заминаҳои эмпирикӣ. Дар раванди таҳқиқот таҷрибаи мақомоти ҳифзи ҳуқуқи Ҷумҳурии Тоҷикистон дар самти муқовимат бо киберҷиноятҳо аз ҷумлаи Прокуратураи генералии Ҷумҳурии Тоҷикистон, омӯзиши зиёда аз 116 парванда аз бойгонии Суди олии Ҷумҳурии Тоҷикистон, маълумотҳои омории Сармаркази таҳлилӣ-иттилоотии Вазорати корҳои дохилии Ҷумҳурии Тоҷикистон, Раёсати муборизаи бар зидди ҷиноятҳои муташаккили ВКД Ҷумҳурии Тоҷикистон, Вазорати адлияи Ҷумҳурии Тоҷикистон, таҷрибаи созмону ташкилотҳои байналмилалӣ, аз ҷумла СММ, Иттиҳоди Байналмилалии Телекоммуникатсия, Интерпол, Европол, Созмони ҳамкории Шанхай ва Созмони паймони амнияти дастаҷамъӣ мавриди таҳлил қарор дода шудаанд.

Навгонии илмии таҳқиқот. Таҳқиқоти мазкур аввалин тадқиқоти диссертатсионии ватанӣ мебошад, ки масъалаҳои назариявӣ ва амалии ҳуқуқи ҷиноятӣ ва масъалаҳои криминологии муқовимат ба киберҷиноятҳоро дар бар мегирад. Бояд гуфт, ки қаблан дар сатҳи тадқиқоти монографӣ ва диссертсионӣ масъалаҳои ҳуқуқии ҷиноятӣ ва криминологии муқовимат ба киберҷиноятҳо муфассал таҳлил карда нашудааст.

Нуктаҳои ба ҳимоя пешниҳодшаванда. Ба ҳимоя нуктаҳои илмии зерин пешниҳод мегарданд, ки онҳо навгониҳои диссертатсияро ифода мекунанд:

1. Киберҷиноятҳо – маҷмуи ҷиноятҳое, ки бо истифода аз воситаҳои барномавӣ-техникӣ ва ТИК дар фазои маҷозӣ бо мақсади ғайриқонунӣ ба даст овардан, тағйир додани иттилоот, несту нобуд ё бекор кардани системаҳо ва захираҳои иттилоотӣ нигаронидашуда, ҷиҳати расонидани зарар ба ҳуқуқу озодиҳои конститутсионии инсон ва шаҳрванд, амнияти давлатӣ ва ҷамъиятӣ ё муносибатҳои молу мулкӣ равона карда шудаанд.

2. Бо дарназардошти он, ки инсоният дар ибтидои асри XXI ба таҳдидҳо ва хатарҳои нави ҷаҳонии иттилоотӣ дучор омад, таъмини амнияти иттилоотӣ аз ҳамлаҳои киберӣ аз ҷумлаи вазифаи мубрами давлати муосир ба ҳисоб рафта таҳдидҳои имрӯзаи иттилоотӣ (ҳамлаҳои киберӣ, воридшавии ғайриқонуни ба системаҳои иттилоотӣ, паҳн намудани барномаҳои зараровар ва вирусҳои компютерӣ) ба амнияти миллии давлат зарари ҷиддӣ мерасонанд.

3. Ташаббусҳои байналмилалии Ҷумҳурии Тоҷикистон дар таъмини амнияти иттилоотӣ аз ҳамлаҳои киберӣ ва муқовимат бо киберҷиноятҳо чунин марҳилаҳоро дар бар мегирад:

– марҳила аввал, соли 1992 дар ш. Тошкенти Ҷумҳурии Ӯзбекистон ба имзо расидани «Созишнома дар бораи таъмини воситаҳои рақамӣ ва амнияти иттилоотӣ» дар байни давлатҳои аъзои Иттиҳоди Давлатҳои Мустақил;

– марҳилаи дуюм 1-уми июни соли 2001 то инҷониб дар шаҳри Мински Ҷумҳурии Белорус имзои «Созишнома дар бораи ҳамкории давлатҳои аъзои ИДМ дар мубориза бар зидди ҷиноятҳо дар соҳаи иттилооти компютерӣ».

4. Дар доираи СПАД «Маркази муқовимат бо киберҷиноятҳо», ҳамчун мақомоти махсусгардонидашуда таъсис дода шуда, ҳадафи таъсиси он ҷамъоварӣ ва коркарди маълумот оид ба киберҷиноятҳо, гузаронидани арзёбии экспертии таҳдидҳои киберӣ, таҳия ва татбиқи усулҳои пешрафтаи пешгирӣ ва тафтиши киберҷиноятҳо, таълими кадрҳои нав, мусоидат ба мақомоти ҳифзи ҳуқуқ, баланд бардоштани дараҷаи бехатарии фазои иттилооти аз ҳамлаҳои киберӣ дар минтақа ва ҷаҳон, инчунин ҳалли масъалаи ҳамкории шаффофи онҳо дар самти дастгирии ташкилии муқовимат бо киберҷиноятҳо муқаррар карда шавад.

5. Бо мақсади огоҳонидан ва пешгирии киберҷиноятҳо дар ҶТ Маркази ягонаи коммутатсионии алоқаи барқии Хадамоти алоқаи назди Ҳукумати ҶТ, Прокуратураи генералии ҶТ ва Вазорати корҳои дохилии ҶТ, дар шароити ҷаҳонишавӣ, инчунин компютеркунонии босуръати тамоми бахшҳои ҳайётан муҳими давлатӣ бо мақсади таъмини амнияти иттилооти аз ҳамлаҳои киберӣ дар мамлакат, дастрасиро ба сомонаҳо ва захираҳои дигари иттилоотӣ, аз ҷумла сомона ва барномаҳои интернетӣ, ки ба паҳн намудани ҳама гуна иттилоот бар зидди асосҳои сохтори конститутсионӣ, амнияти шахсӣ, ҷамъиятӣ, давлатӣ, иттилоот дар бораи маҳдуднамоии ҳуқуқу

озодиҳои инсон ва шаҳрванд, барангехтани кинаю адовати динию мазҳабӣ ё низои миллӣ, нажодӣ, маҳалгароӣ, тарзи омодасозӣ ва тарғиби маводи нашъаовар, тарканда ва маводи дигари заҳролудкунанда, ба содир намудани ҷиноят ва ҳуқуқвайронкунии маъмурӣ равонагардида, хусусияти экстремистию террористидошта, порнография, аз ҷумла порнографияи кӯдакона, инчунин паҳн намудани ҳама гуна маълумот, ки бо санади судии эътибори қонунӣ пайдонамуда ки қонунгузории Ҷумҳурии Тоҷикистон манъ кардааст, маҳдуд намоянд.

6. Дар маҷмуъ киберҷиноятҳоро аз рӯйи асосҳои зерин тасниф кардан мумкин аст:

а) вобаста ба объекти таҷовузи ҷиноятӣ: таҷовуз ба ҳуқуқ ва манфиатҳои соҳибони иттилооти компютерӣ; таҷовуз ба ҳуқуқ ва манфиатҳои соҳибони воситаҳои иттилоот;

б) аз рӯйи хусусияти зараре, ки ба иттилооти компютерӣ мерасонад: барномаҳои зараррасони тағйирдиҳанда, нобудкунанда, маҳкамкунанда, корношоямкунанда, нусхабардорикунандаи итилооти компютерӣ;

в) вобаста ба усулҳои содир намудани ҷиноят: ирсоли мактубҳо бо роҳи фиреб; содиршавии онҳо тавассути интернет.

7. Танзими ҳуқуқии ҷавобгарии ҷиноятӣ барои киберҷиноятҳо дар давлатҳои хориҷӣ ва пасошуравӣ ба таври гуногун ба роҳ монда шудааст:

– объекти таҷовуз ҳангоми содир шудани киберҷиноятҳо дар қонунгузории ҷиноятии давлатҳои пасошуравӣ ва кишварҳои хориҷӣ на танҳо муносибатҳои ҷамъиятӣ дар соҳаи муомилоти бехатари иттилооти компютерӣ (КҶ ҶТ), балки дигар объектҳо низ мебошанд (масалан, ҳуқуқ ва озодиҳои конститутсионии инсон ва шаҳрванд озодӣ ва сулҳи умум – қонунгузории ҷиноятии Франсия ва Олмон, амнияти миллӣ ва фаъолияти муътадили иқтисодӣ – қонунгузории ҷиноятии ШМА, тартиботи ҷамъиятӣ ва амнияти ҷамъятӣ –қонунгузории ҷиноятии Қазоқистон);

– муайян карда шудааст, ки дар қонунгузори ҷиноятии давлатҳои хориҷ субъекти ҷиноятҳо ба муқобили амнияти киберӣ ба ду гурӯҳ тақсим карда мешаванд: давлатҳое, ки ба сифати субъекти ҷинояти мазкурро танҳо шахси воқеии мукаллафи ба синну соли муқарраршуда расида, дар баъзан ҳолатҳо субъекти махсус баромад мекунад, (Ҷумҳуриҳои Қирғизистон, Ӯзбекистон, Қазоқистон ва ғ.); давлатҳое, ки ба сифати субъекти ин ҷиноятҳо дар баробари шахси воқеи ҳамчунон шахсони ҳуқуқиро эътироф мекунанд (Дания, Латвия, Литва, Молдавия, Франсия, Шветсия, Эстония ва ғайра);

– вобаста ба муқаррар кардани ин ҷиноятҳо дар қонунгузории ҷиноятии давлатҳои хориҷӣ муқаррароти гуногун дида мешавад. Дар як гурӯҳ давлатҳо (масалан, ҶМ Чин) барои аз ҷониби субъектони махсус иҷро нагардидани қарорҳои субъектони муборизабаранда бо киберҷиноятҳо оид ба бастани захираҳои интернетии дахлдор ва нест кардани маълумоти манъшуда, мусоидати маҷозӣ (виртуалӣ) барои содир намудани киберҷиноятҳо, истифодаи захираҳои интернетӣ бо мақсади паҳн кардани маълумот дар бораи усулҳои

содир намудани ҷиноят ҷавобгарии ҷиноятиро пешбинӣ шудааст. (м. 285А, 286А, 287А, 287В). Дар баъзан давлатҳо бошад, ҷиноятҳое, ки бо истифода аз ТИК содир мешаванд, аз ҷумла қаллобии интернетӣ ҷавобгарии ҷиноятиро муқарар намудаанд. (Ҷумҳурии Молдова, ФР, Британияи Кабир, Испания, Белгия, Дания, Эстония ва ғ.).

8. Объекти ҷиноятҳо муқобили шабакаҳои интернетӣ ва таҷҳизотҳои ёрирасони онҳо**:** (барномаҳои зарраровар ва ҳамлаҳои DoS)-ро муносибатҳои ҷамъиятӣ дар самти ҷиноятҳо муқобили амнияти иттилоотӣ (муомилоти бехатари иттилооти компютерӣ аз ҳамлаҳои киберӣ), инчунин манфиатҳои гуногуни шахсӣ ва иҷтимоӣ (ҳаёт, саломатӣ, молу мулк, дигар арзишҳои моддӣ ва ғайримоддӣ) ва ҳуқуқ ва манфиатҳои қонунан ҳифзшавандаи субъектони муносибатҳои ҳуқуқӣ (шахсони воқеию ҳуқуқӣ ва мақомоти маҳаллии ҳокимияти давлатӣ) ташкил медиҳанд.

9. Асосонок карда мешавад, ки объектҳои ҷиноятҳо муқобили шабакаҳои интернетӣ ба гуруҳҳои зерин тақсим карда шавад:

– объекти намудии ҷиноятҳо муқобили шабакаҳои интернетӣ ва таҷҳизотҳои ёрирасони онҳо (барномаҳои зарраровар ва ҳамлаҳои DoS)-ро, муносибатҳои муҳими ҷамъиятии бо қонунгузории ҷиноятӣ ҳифзшаванда дар соҳаи бехатарии таҳия, истифода ва паҳнкунии иттилооти компютерӣ, захираҳои иттилоотӣ, системаҳои иттилоотӣ ва ТИК, ҳуқуқ ва манфиатҳои шахсонӣ воқеӣ ва ҳуқуқӣ, ҷамъият ва давлат оид ба истифодаи системаи автоматикии коркарди маълумот ташкил медиҳад.

– объекти бевоситаи ҷиноятҳо муқобили шабакаҳои интернетӣ ва таҷҳизотҳои ёрирасони онҳо вобаста ба хусусияти худ ҳамчун намуди киберҷиноятҳо фарогири ду объект мебошад:

а) объекти асосии ин ҷиноятҳо бевосита муносибатҳои ҷамъиятие мебошанд, ки ҳуқуқ ва манфиатҳои қонунии соҳибони иттилооти компютерӣ ва танзимгарони системаҳои иттилоотиро дар соҳаи таҳия, коркард, соҳибӣ кардан, паҳн кардан, пешниҳод кардан, истифодаи иттилооти компютерӣ, фаъолияти бехатари компютерҳо, системаҳои компютерӣ, шабакаҳои компютерӣ, системаҳои иттилоотӣ ва шабакаҳои иттилоотию телекоммуникатсионӣ таъмин менамоянд.

б) объекти иловагии ин ҷиноятҳо муносибатҳои ҷамъиятие мебошанд, ки бо меъёрҳои ҳуқуқ танзим шуда, ҳуқуқ ва манфиатҳои қонунии шахс, ҷомеа ва давлатро таъмин мекунанд.

10. Аз баррасӣ ва таҳлили объекти ҷиноятҳо муқобили шабакаҳои интеренти ва таҷҳизотҳои ёрирасони онҳо бар меояд, ки кирдорҳои барои ҷамъият хавнок (баронмаҳои зараровар, ҳамлаҳои DoS) на танҳо ба амнияти иттилоотӣ, балки ба муносибаҳои гуногуни ҷамъиятӣ зарар мерасонанд ва таҳдиди расонидани чунин зарарро ба миён меоранд. Қонунгузории ҷиноятии ватанӣ категорияи ҷинояти мазкурро дар боби 28 «Ҷиноятҳо ба муқобили амнияти иттилоотӣ» пешбинӣ намудааст, ва бо дарназардошти дигар муносибатҳои ҷамъиятиро дар бар гирифтани ин боб (кибертерроризм,

киберэкстремизм, кибертаъқиб, мактуби фишигӣ ва ғ.) мувофиқи мақсад мешуморем, фасли нав дар КҶ ҶТ бо номи « Ҷиноятҳо муқобили амнияти киберӣ» ворид карда шавад.

11. Ба фасли нави «Ҷиноятҳо муқобили амнияти киберӣ» бобҳои зеринро шомил мебошанд: ҷиноятҳо муқобили шабакаҳои интернетӣ ва таҷҳизотҳои ёрирасони онҳо (киберҷиноятҳои харобиовар); ҷиноятҳое, ки бо истифодаи шабакаи интернет ва захираҳои электронии иттилоотӣ (шабакаҳои иҷтимоӣ мессенҷерҳо ва дигар захираҳо) содир мешаванд; ҷиноятҳое, ки бо истифодаи воситаҳои гуногуни техникӣ содир мешаванд; ҷиноятҳое, ки ҳаёт ва саломатиро дучори хатар мегузоранд; ҷиноятҳое, ки махфияти иттилоотро вайрон мекунанд аз ҷумла дастрасии ғайриқонунӣ ба компютерҳо ё системаҳои компютерӣ бидуни расонидани зарар ба иттилоот.

12. Ба сифати субъекти ҷиноятҳое, ки ба муқобили шабакаҳои интернетӣ ва таҷҳизотҳои ёрирасони онҳо (барномаҳои зараровар, ҳамлаҳои DoS) равона гардидааст, дилхоҳ шахси воқеӣ ва мукаллаф шуда метавонад (яъне субъекти умумии ҷиноят), ки дар вақти содир кардани ҷиноят ба синни 14 расидааст. Шахсони синни 14-19-сола дар даврони муосир истифодабарандагони шабакаи «Интернет» ва соҳиби дастгоҳҳои компютерӣ (телефонҳои мобилӣ, смартфонҳо, ноутбукҳо, планшетҳо ва ғайра) буда, дониш, маҳорат ва малакаҳои зарурии кор бо ТИК-ро доро мебошанд. Бинобар ин, онҳо барои иҷро намудани тарафи объективии таркиби ҷинояти барраасишаванда аз нигоҳи назариявӣ ва амалӣ имкон доранд. Зарур мешуморем, ки ба қисми 2-и моддаи 23-и Кодекси ҷиноятии Ҷумҳурии Тоҷикистон (оид ба синну соли ҷавобгарии ҷиноятӣ) бо таркиби ҷиноятҳое, ки дар моддаҳои 300 ва 303-и Кодекси ҷиноятии Ҷумҳурии Тоҷикистон пешбинӣ шудаанд, илова ворид карда шавад ва ҷавобгарии ҷиноятӣ барои ин гуна ҷиноятҳо аз синни 14-солагӣ муқаррар карда шавад.

13. Тарафи объективии ҷиноятҳое, ки тавассути воситаҳои гуногуни техникӣ содир мешаванд, маҷмуи аломатҳоеро дар бар мегирад, ки муносибатҳои зоҳирии шахсро вобаста ба ҷамъоварии ғайриқонунии маълумот дар бораи шахси дигар, паҳн кардани маълумот дар доираи васеъ, ба таври оммавӣ ва ё дар воситаҳои ахбори омма намоиш додани маълумот, инчунин ирсоли мактубҳо бо роҳи фиреб ҳангоми истифода аз шабакаи интернет, ки расонидани зарар ба ҳуқуқ ва манфиатҳои қонунии ҷабрдидаро ба вуҷуд меорад ташкил медиҳад.

Пешниҳодҳо ҷиҳати такмили қонунгузорӣ:

14. Аз тарафи муаллиф лоиҳаи Қонуни Ҷумҳурии Тоҷикистон «Дар бораи амнияти киберӣ» пешниҳод карда шуда, дар он бо мақсади таъмини амнияти иттилоотӣ аз ҳамлаҳои киберӣ муқаррароти умумӣ оид ба амали қонун, танзими давлатии амнияти киберӣ, ҳуқуқ ва ӯҳдадориҳои мақомоти давлатӣ ва ташкилотҳои давлатӣ оид ба таъмини амнияти киберӣ, таъмини амнияти киберӣ, ҳодисаҳои амнияти киберӣ, объектҳои инфрасохтори муҳими иттилоотӣ, дастгирӣ ва рушди таъмини амнияти киберӣ, ҳамкории

байналмилалӣ дар самти амнияти киберӣ ва дигар самтҳои муҳими танзими ҳуқуқӣ пешбинӣ карда шаванд.

15. Бо мақсади такмили қонунгузории ҷиноятӣ ва мустаҳкам гардонидани меъёрҳои боби 28 КҶ ҶТ чунин пешниҳодҳоро вобаста ба тағйиру иловаҳо дар қонунгузории ҷиноятӣ зарур мешуморем.

Моддаи 298 (1) Ба даст овардани маълумоти электронии шахсӣ бо роҳи фиреб ё усулҳои дигари дастрасии ғайриқонунӣ ба маълумот барои истифода ба манфиати шахсӣ

1. Ба даст овардани маълумоти электронии шахсӣ тавассути шабакаи интернет бо роҳи фиреб ё усулҳои дигари дастрасии ғайриқонунии маълумот бо мақсади истифода ба манфиати шахсӣ, -

бо... ҷазо дода мешавад.

2. Ҳамин кирдор, агар боиси расонидани зарари калон гардида бошад, бо ... ҷазо дода мешавад.

3. Кирдорҳои пешбининамудаи қисмҳои якум ё дуюми ҳамин модда агар, ки аз ҷониби гурӯҳи шахсон бо созиши пешакӣ ё аз ҷониби гурӯҳи муташаккил ва ё шахсе бо сӯистифода аз мақоми хизматиаш содир карда шудаанд, бо ... ҷазо дода мешавад.

4. Кирдорҳои пешбининамудаи қисмҳои якум, дуюм ва сеюми ҳамин модда агар боиси оқибатҳои вазнин гардида бошанд ё хатари сар задани онҳоро ба миён оварда бошанд, пас бо ... ҷазо дода мешавад.

16. Зарур мешуморем, ки ба моддаи 300 Кодекси ҷиноятии ҶТ, қисми 2 дар таҳрири зерин илова карда шавад:

«Ҳамин кирдор агар:

в) бо мақсади авбошӣ содир шуда бошанд;

г) бо мақсади тарсонидани аҳолӣ ё таъсир расонидан ба қабули қарорҳои мақомоти давлатӣ ва (ё) худидоракунии маҳаллӣ содир шуда бошанд;

д) бо мақсади монеъ шудан ба фаъолияти муътадили воситаҳои ахбори омма, мақомоти ҳокимияти давлатӣ ва (ё) худидоракунии маҳаллӣ, муассисаҳои давлатӣ содир шуда бошанд»;

17. Пешниҳод карда мешавад, ки дар боби 28-и КҶ ҶТ моддаҳои нав, (моддаҳои 300 (1) ва 300 (2)) бо мазмуни зайл ворид карда шавад:

Моддаи 300 (1) Ҳамлаи компютерии DoS

1) Ҳамлаи компютерии DoS, таъсири ҳадафнок ба системаи ё шабакаи компютерӣ бо истифода аз барномаҳои зараровар, ки ба халалдор кардани фаъолияти он нигаронида шуда, дар натиҷа корбаронро аз имкони дастрасӣ ба манбаи электронии дархостшуда маҳрум мекунад,-

бо... ҷазо дода мешавад.

Моддаи 301 (2) Ғайриқонунӣ дар шакли оммавӣ паҳн кардани паёмҳои электронӣ

1) Ба таври оммавӣ ғайриқонунӣ паҳн кардани паёмҳои номатлуб, – фиристодани мактубҳои оммавии хусусияти таблиғотии экземистӣ,

террористӣ тавассути шабакаи интернетӣ ё бо роҳи истифодаи алоқаи телефонӣ, факс, радио, телефони мобилӣ, аз ҷумла бо истифода аз воситаҳои интихоб ва (ё) занг задан ба рақами абонентӣ, -

бо … ҷазо дода мешавад.

2) Ҳамин кирдор, ки аз ҷониби гурӯҳи шахсон бо созиши пешакӣ содир шуда бошад, -

бо... ҷазо дода мешавад.

3) Кирдори дар кисмҳои якум ё дуюми ҳамин модда пешбинишуда, ки аз ҷониби гурӯҳи муташаккил ва ё бо истифода аз мақоми хизматӣ содир шуда бошад, -

бо ... ҷазо дода мешавад.

18. Бо мақсад мувофиқ аст, ки қисми 3-юми моддаи 301 КҶ ҶТ бандҳои алоҳида ба таври зайл илова карда шавад:

д) боиси нобудшавӣ ва ё басташавӣ, иттилоот гардида бошад;

е) аз ҷониби шахсе, ки аз мақоми хизматиаш истифода мебарад, инчунин аз ҷониби шахсе, ки ба компютер, системаи компютерӣ ё шабакаи онҳо дастрасӣ дошта бошад, содир шуда бошад.

Ҳамзамон зарур аст, ки бо назардошти ҳифзи тартиботи ҷамъиятӣ ва арзишҳои ахлоқию фарҳагӣ, моддаи 301 (3) ба КҶ ҶТ дар мазмуни зерин ворид карда шавад:

Моддаи 301 (3). Таҳия, интишор ва паҳн кардани иттилоот, бо истифодаи шабакаи интернет ва ҳама гуна воситаҳои шабакаҳои иттилоотию телекоммуникатсионӣ

1) Таҳия, интишор ва паҳн кардани иттилоот, бо истифодаи шабакаи интернет ва ҳама гуна воситаҳои шабакаҳои иттилоотию телекоммуникатсионӣ, ки боиси халалдор гардидани тартиботи ҷамъиятӣ, арзишҳои ахлоқию фарҳагӣ мегардад,-

бо ... ҷазо дода мешавад.

19. Асоснокии хулосаи муаллиф бо назардошти таҳлили қонунгузории ҷиноятии давлатҳои хориҷӣ ва пасошуравӣ зарурияти ворид намудани тағйирот ба қисми 2 моддаи 302 КҶ ҶТ-ро ба миён оварад:

2) Ҳамин кирдор агар ба ҳудуди Ҷумҳурии Тоҷикистон ворид намудан, тайёр, паҳн кардан ва истифодаи намудҳои гуногуни таҷҳизот ва барномаҳоро, ки барои дигаргун кардани маълумоти идентификаторҳо истифода мешаванд, -

бо ... ҷазо дода мешавад.

20. Пешниҳод карда мешавад, ки моддаи 303-и Кодекси ҷиноятии Ҷумҳурии Тоҷикистон дар таҳрири зайл ифода карда шавад:

Моддаи 303. Ғайриқонунӣ таҳия, истифода ё паҳн кардани барномаҳои зараровари компютерӣ

1) Таҳияи барномаҳои компютерӣ, ворид намудани тағйирот ба барномаи мавҷуда, бо мақсади ғайриқонунӣ нобуд кардан, муҳосира, тағйир додан, нусхабардорӣ намудан, истифодаи иттилооти дар ҳомили электронӣ

нигоҳдошташаванда, ки дар низоми иттилоотӣ маҳфузанд, ё тавассути шабакаҳои телекоммуникатсионӣ интиқол дода мешаванд, вайрон кардани кори компютер, дастгоҳи абонентӣ, барномаи компютерӣ, низоми иттилоотӣ, ё шабакаҳои телекоммуникатсионӣ, ҳамчунин, қасдан истифода ва (ё) паҳн намудани чунин барномаҳо, -

бо ... ҷазо дода мешавад.

2) Ҳамин кирдор, ки агар бо расонидани зарари калон ба шаҳрвандон содир шуда бошанд, -

бо ... ҷазо дода мешавад.

3) Кирдорҳои пешбининамудаи қисмҳои якум ё дуюми ҳамин модда, агар ба андозаи калон содир шуда бошанд, -

бо ... ҷазо дода мешавад.

4) Кирдорҳои пешбининамудаи қисми якум ва дуюми ҳамин модда агар бо истифода аз мақоми хизматӣ содир шуда бошанд, -

бо ... ҷазо дода мешавад.

Аҳаммияти назариявӣ ва амалии таҳқиқот. Аҳаммияти назариявӣ ва амалии таҳқиқот дар он ифода мегардад, ки хулосаҳои назариявиро, ки дар натиҷаи таълифи таҳқиқоти диссертатсионӣ ба даст оварда шудаанд, метавон дар омӯзиши минбаъдаи масъалаҳои назариявӣ ва амалии киберҷиноятҳо дар Ҷумҳурии Тоҷикистон ва дигар давлатҳои хориҷ истифода бурд. Натиҷаҳои таҳқиқот дар фаъолияти қонунгузорӣ ва мақомоти ҳифзи ҳуқуқ (КДАМ, Вазорати корҳои дохилии ҶТ, Прокуратураи генералии Ҷумҳурии Тоҷикистон, Вазорати адлияи ҶТ) ва судҳо метавонанд истифода карда шаванд. Ғайр аз ин, ба мақсад мувофиқ аст, ки натиҷаҳои таҳқиқот ҷиҳати мукаммалгардонии фаъолияти мақомоти ҳифзи ҳуқуқ дар самти таъмини амнияти иттилоотӣ аз ҳамлаҳои киберӣ, дар шароити ҷаҳонишавӣ истифода бурда шавад. Маводи таҳқиқоти диссертатсионӣ метавонад дар фаъолияти омӯзгорӣ барои таълими фанҳои таълимии «Ҳуқуқи ҷиноятӣ», «Ҳуқуқи ичрои ҷазои ҷиноятӣ» ва «Криминология», ҳамзамон барои гузаронидани семинарҳо, конфронсҳо ва «мизҳои мудаввар»-и илмӣ ва корҳои амалӣ муфид хоҳанд буд.

Дараҷаи эътимоднокии натиҷаҳои таҳқиқот. Асарҳои нашршудаи муаллифро омӯзгорони муассисаҳои таълимӣ, ва мақомотҳои ҳифзи ҳуқуқи кишавр аз ҷумла дар Академияи Вазорати корҳои дохилии Ҷумҳурии Тоҷикистон, факултети ҳуқуқшиносии Донишгоҳи миллии Тоҷикистон, Донишгоҳи славянии Россия ва Тоҷикистон, дар Маркази миллии қонунгузории назди Президенти ҶТ, шуъбаи мубориза бо ҷиноятҳои кибернетикии Прокуратураи генералии Ҷумҳурии Тоҷикистон, шуъбаи экспертизаи судӣ техникаи-компютерӣ ва видео-овозшиносии Маркази ҷумҳуриявии экспертизаи судӣ ва криминалистии Вазорати адлияи Ҷумҳурии Тоҷикистон, ҳангоми хондани лексияҳо ва гузаронидани машғулиятҳои семинарӣ (амалӣ) бо донишҷӯён, магистрантҳо ва аспирантҳо, ҳангоми такмили ихтисоси кормандони мақомоти ҳифзи ҳуқуқ истифода мебаранд.

Мутобиқати диссертатсия ба шиносномаи ихтисоси илмӣ. Диссертатсияи таҳқиқшуда ба шиносномаи ихтисоси илмӣ 12.00.08 – Ҳуқуқи ҷиноятӣ ва криминология; ҳуқуқи иҷрои ҷазои ҷиноятӣ, ки аз ҷониби Комиссияи олии аттестатсионии назди Президенти Ҷумҳурии Тоҷикистон тасдиқ шудааст[50], мувофиқат мекунад.

Саҳми шахсии довталаби дараҷаи илмӣ дар таҳқиқот дар он зоҳир мегардад, ки таҳқиқоти диссертатсионӣ бевосита аз ҷониби муаллиф иҷро шудааст, дар доираи пажуҳиш мафҳумҳои асосӣ шарҳ дода шуда, тамоюлҳои нав ошкор карда шудаанд, падидаҳои нави ҳамкориҳои байналмилалӣ дар муқовимат бо киберҷиноятҳо муайян гардида, роҳҳои ҳалли проблемаҳои мубрами дар ин самт ҷойдошта дар доираи муқаррароти илмӣ нишон дода шудаанд, хулосаҳо ва пешниҳодҳо дар интишороти илмии муаллиф аз рӯйи мавзуи таҳқиқи диссертатсионӣ дарҷ гардидаанд. Инчунин вобаста ба масъалаи таҳқиқшаванда довталаб дар чандин чорабиниҳои илмию амалии сатҳи гуногун баромад намуда, ҷиҳати такмили донишҳои назариявӣ ва баланд бардоштани малакаи касбии кормандони мақомоти прокуратура санаҳои 22-31 августи соли 2022 дар се минтақа бо иштироки 68 прокуророни шаҳру ноҳияҳо ва прокуророни ба онҳо баробаркардашуда дар шаҳри Душанбе, вилоятҳои Суғду Хатлон дар бораи натиҷаҳои таҳқиқот маълумот дода, хулосаҳои ҳуқуқии зарурӣ ва мушкилоту камбудиҳои ҷойдошта аз рӯйи таҷрибаи тафтишотӣ-судӣ, истифодаи воситаҳои техникаи муосир, масъалаҳои ҳуқуқӣ-ҷиноятӣ ва криминологии муқовимат бо киберҷиноятҳо, тартиб ва тарзу усули баамалбарории тафтишии ин намуди ҷиноятҳоро пешниҳод намудааст[51]. Муаллифи асарҳои зиёди илмию таълимӣ оид ба мавзуи интихобкардааш мебошад.

Тасвиб ва амалисозии натиҷаҳои диссертатсия. Диссертатсия дар кафедраи криминалистика ва фаъолияти экспертизаи судии факултети ҳуқуқшиносии ДМТ иҷро шуда, якчанд маротиба дар ҷаласаҳои он муҳокима шуда, баъдан ба ҳимоя дар Шурои диссертатсионии 6D. КОА-019 назди ДМТ тавсия шудааст. Натиҷаҳои алоҳидаи таҳқиқоти диссертатсионӣ дар конференсияҳои ҳарсолаи ҷумҳуриявии илмӣ-назариявӣ (амалӣ)-и устодон (ҳайати профессорону устодон) ва кормандони ДМТ (солҳои 2017-2023), инчунин хулосаву пешниҳодҳо дар конференсияҳои зерини байналмилалӣ ва ҷумҳуриявӣ дар шакли маъруза ироа гардидаанд:

а) байналмилалӣ:

– Конференсияи байналмилалии илмию амалӣ дар мавзуи «Ҳуқуқи инсон: дирӯз ва имрӯз» – маъруза дар мавзуи «Проблемаҳои муқовимат бо ҷиноятҳои компютерӣ ҳамчун як шакли мушаххаси киберҷиноятҳо» (Душанбе, ДМТ, 9 декабри соли 2022);

[50] Ниг.: Қарори Раёсати Комиссияи олии аттестатсионии назди Президенти Ҷумҳурии Тоҷикистон аз 30 сентябри соли 2021, таҳти №7 // Бюллетени Комиссияи олии аттестатсионии назди Президенти Ҷумҳурии Тоҷикистон. – 2022. – №1-2 (21-22). – С. 82, 144.

[51] Ниг.: Мактуби Прокурори генералии Ҷумҳурии Тоҷикистон аз 11.08.2022, таҳти №32/3-145.

– Конференсияи байналмилалии «Илм ва таҳсилот: тамоюлҳои рушд дар ҷомеаи иттилоотӣ» бахшида ба «75-солагии Донишгоҳи миллии Тоҷикистон» – маъруза дар мавзуи «Ташаббусҳои байналмилалии Ҷумҳурии Тоҷикистон дар таъмини амнияти иттилоотӣ аз ҳамлаҳои киберӣ» (Душанбе, ДМТ, 20-21 октябри соли 2023);

– Конференсияи илмӣ-амалии байналмилалӣ дар мавзуи «Тоҷикон дар оинаи таърих», бахшида ба 115 солагии академик Бобоҷон Ғафуров – маъруза дар мавзуи «Таҳдидҳои киберӣ: қаллобӣ дар фазои маҷозӣ» (Душанбе, Филиали Донишгоҳи давлатии Москва ба номи Михаил Ломоносов дар шаҳри Душанбе, 27 октябри соли 2023);

– Конференсияи илмӣ-амалии байналмилалӣ дар мавзуи «25-солагии Кодекси ҷиноятии Ҷумҳурии Тоҷикистон: вазъият ва дурнамо» – маъруза дар мавзуи «Ташкилотҳои байналмилалӣ ҳамчун субъектони муқовимат бо киберҷиноятҳо». (Душанбе, Академияи Вазорати корҳои дохилии ҶТ, 26 майи соли 2023);

– Конференсияи байналмилалии илмӣ-амалӣ дар мавзуи «Ҳифзи ҳуқуқи инсон ва масъалаи муқовимат ба коррупсия дар ҷаҳони муосир: консепсияҳо, воқеият ва дурнамо» – маъруза дар мавзуи «Интернет воситаи содиршавии кибертаъқиб» (Душанбе, Академияи идоракунии давлатии назди Президенти Ҷумҳурии Тоҷикистон, 1-2 декабри соли 2023);

– Конференсияи байналмилалии илмию назариявӣ дар мавзуи «Масъалаҳои назариявии ташаккули фарҳанги ҳуқуқи инсон дар Тоҷикистон» – маъруза дар мавзуи «Таҳлили таҷрибаи амалии мақомоти ваколатдори давлатӣ ва ҳамкории байналмилалии онҳо дар самти таъмини амнияти киберӣ» (Душанбе, ДМТ, 9 декабри соли 2023).

б) ҷумҳуриявӣ:

– Конференсияи ҷумҳуриявии илмӣ-амалӣ дар мавзуи «Криминалистикаи муосир» – маъруза дар мавзуи «Нақши тафакурри сунъӣ дар раванди амалишавии фаъолиятӣ оперативӣ-ҷустуҷӯӣ» (Душанбе, Академияи ВКД ҶТ, 31 декабри соли 2021);

– Конференсияи илмӣ-амалии ҷумҳуриявӣ дар мавзуи «Сиёсати оперативӣ-ҷустуҷӯӣ оид ба таъмини амнияти Ҷумҳурии Тоҷикистон» – маъруза дар мавзуи «Таҳқиқоти ҳуқуқӣ-ҷиноятии мафҳуми киберҷиноятҳо» (Душанбе, Академияи ВКД ҶТ, 4 октябри соли 2022);

– Конференсияи ҷумҳуриявии илмию назариявии «Рушди фаъолияти ҳифзи ҳуқуқ дар Ҷумҳурии Тоҷикистон» – маъруза дар мавзуи «Нақши мақомоти ҳифзи ҳуқуқ дар мубориза бо киберҷиноятҳо» (Душанбе, ДМТ, 6 октябри соли 2022);

– Конференсияи ҷумҳуриявии илмию назариявӣ дар мавзуи «Нақши Конститутсия дар амалишавии ҳадафҳои стратегии давлат» – маъруза дар мавзуи «Киберҷиноятҳо: таҳдидҳои асри XXI» (Душанбе, ДМТ, 1 ноябри соли 2022);

– Конференсияи ҷумҳуриявии илмӣ-назариявӣ дар мавзуи «Конститутсияи Ҷумҳурии Тоҷикистон ва низоми ҳуқуқии миллӣ» – маъруза дар мавзуи «Киберҷиноятҳо ҳамчун омили таҳдидкунанда ба амнияти ҷомеа» (Душанбе, Академияи ВКД ҶТ, 3 ноябри соли 2022);

– Конференсияи илмӣ-амалии ҷумҳуриявӣ дар мавзуи «Мушкилоти қонунгузории замини Ҷумҳурии Тоҷикистон дар замони муосир» – маъруза дар мавзуи «Барномаҳои зараровар ҳамчун воситаи содиршавии киберҷиноятҳо: мафҳум ва намудҳои он» (Душанбе, ДМТ, 13 октябри соли 2023);

– Конференсияи илмӣ-амалии ҷумҳуриявӣ дар мавзуи «Муқовимат ба савдои одамон: Мушкилот ва мулоҳизаҳо» – маъруза дар мавзуи «Интернет ва шабакаҳои иҷтимоӣ: воситаи содиршавии савдои одамон» (Душанбе, «Китобхонаи миллии Тоҷикистон» 26 октябри соли 2023);

– Конференсияи илмӣ-назариявии ҷумҳуриявӣ дар мавзуи «Масоили мубрами такмили Конститутсияи Ҷумҳурии Тоҷикистон дар шароити муосир» – маъруза дар мавзуи «Хакер: тавсифи криминологии он» (Душанбе, ДМТ, 1 ноябри соли 2023).

Муқаррароти алоҳидаи диссертатсия аз ҷониби муаллиф ҳангоми хондани лексия аз фанни таълимии «Асосҳои тафтиши киберҷиноятҳо» (барои муҳассилини ихтисоси санҷишии судӣ) дар факултети ҳуқуқшиносии Донишгоҳи миллии Тоҷикистон истифода шудаанд. Илова бар ин, натиҷаҳои таҳқиқот дар фаъолияти қонунгузории Маҷлиси миллии Маҷлиси Олии ҶТ, фаъолияти шуъбаи мубориза бо ҷиноятҳои кибернетикии Прокуратураи генералии Ҷумҳурии Тоҷикистон, шуъбаи экспертизаи судӣ техникаи-компютерӣ ва видео-овозшиносии Маркази ҷумҳуриявии экпертизаи судӣ ва криминалистии Вазорати адлияи Ҷумҳурии Тоҷикистон, мавриди корбурд қарор гирифтаанд.

Интишорот аз рӯйи мавзуи диссертатсия. Оид ба муҳтавои диссертатсия муаллиф 28 мақолаи илмӣ, аз ҷумла 20 мақола дар нашрияҳои тақризшавандаи Комиссияи олии аттестатсионии назди Президенти ҶТ ва 8 мақола дар нашрияҳои дигар бо забонҳои тоҷикӣ ва русӣ интишор шудаанд. Ҳамчунин муаллифи 1 воситаи таълимӣ низ мебошад, ки масъалаҳои таҳлилшуда ба мавзуи диссертатсия алоқаманд мебошанд. Ҳамин тавр, ҳаҷми умумии интишороти довталаб зиёда аз 85 ҷузъи чопӣ мебошанд.

Сохтор ва ҳаҷми диссертатсия ба мавзуъ ва объектҳои таҳқиқот, мақсаду вазифаҳои гузошташуда мувофиқат мекунад. Диссертатсия аз аз номгӯйи ихтисораҳо ва (ё) аломатҳои шартӣ, муқаддима, панҷ боб, понздаҳ зербоб, хулоса, тавсияҳо оид ба истифодаи амалии натиҷаҳои таҳқиқот, рӯйхати адабиёт (маъхазҳо) ва феҳристи интишороти илмии довталаби дарачаи илмӣ иборат мебошад. Ҳаҷми диссертатсияро 480 саҳифа ташкил медиҳад.

ҚИСМҲОИ АСОСИИ ТАҲҚИҚОТ (ФИШУРДА)

Дар **муқаддима** мубрамии мавзуи таҳқиқи диссертатсионӣ асоснок карда шуда, дараҷаи коркарди илмии он нишон дода шудааст, мақсад ва вазифаҳои кори диссертатсионӣ муайян шуда, объект ва предмет, асосҳои методологӣ ва таҷрибавии таҳқиқот, аҳаммияти назариявӣ ва амалии пажуҳиш муайян ва унсурҳои асосии навгонӣ, нуктаҳои ба ҳимоя пешниҳодшаванда оварда шудаанд.

Дар боби якуми диссертатсия «**Проблемаҳои назариявии муқовимат бо киберҷиноятҳо»** масаълаҳои таҳаввулоти вирусҳои компютерӣ ҳамчун омили асосии ташаккули киберҷиноятҳо, мафҳуми киберҷиноятҳо ва таснифи киберҷиноятҳо мавриди омузиш ва таҳқиқоти илмӣ қарор гирифтааст.

Дар зербоби якуми боби якум **«Таҳаввулоти вирусҳои компютерӣ ҳамчун омили асосии ташаккули киберҷиноятҳо»** диссертант зикр менамояд, ки дар ҷаҳони муосир масъалаҳои таъмини амнияти иттилоотӣ аз ҳамлаҳои киберӣ, аз ҷумла тавассути қонунгузории ҷиноятӣ ба танзим даровардани ин самти ҳаётан муҳим, аз масъалаҳои мубрам ба ҳисоб меравад. Усулҳои муосири коркарди иттилоот бо воситаи техникаи компютерӣ ва дастрасии васеи технологияи компютерӣ имкон доданд, ки онҳо на танҳо барои мақсадҳои илмӣ, тадқиқотӣ ва таълимӣ, балки дар тамоми соҳаҳои ҳаёти ҷамъиятӣ истифода шаванд.

Дар рисола зикр карда шудааст, ки марҳилаи аввали пайдоиши вирусҳои компютерӣ, ҳамчун воситаи содир намудани киберҷиноятҳо замоне, ки вируси Creeper (солҳои 1960-1970) дар шабакаи ҳарбии компютерии Амрико ARPANET (INTERNET) кашф шуд, оғоз ёфт. Барои нест кардани вируси мазкур аввалин барномаи антивирусии Reeper ихтироъ карда шуд. Таъиноти вируси ARPANET (INTERNET) дар он буд, ки вирусҳои зарароварро ошкор ва безарар намуда сипас ба таври дахлдор худ низ нобуд мегардид. Бинобар сабаби махфӣ будани он, аз ҷониби департаменти низомии ИМА, дар бораи ин ҳодиса то ҳол маълумоти дастрас ва боэътимод мавҷуд нест . Дар ин марҳила яке аз аввалин киберҷиноятҳо дар ИМА, охири солҳои 70-ум содир шуда буд. Мушовири амнияти компютерии бонки Security Pacific National Bank Стэнли Рифкин, ки низоми бонкии Лос-Анҷелесро назорат мекард, рамзеро ифшо кард, ки тавассути барномаҳои махсуси компютерӣ ба суратҳисобаш 10 миллион доллларро ворид кард. Содир гардидани ҷинояти мазкур диққати махсуси олимонро ба самти амнияти иттилоотӣ ва муқовимат киберҷиноятҳо чалб намуд .

Хулосабарори карда шудааст, ки таҳқиқоти марҳилаи аввали пайдоиши вирусҳои компютерӣ ҳачун омили асосии содиршавии киберҷиноятҳо, дар як қатор кишварҳои ғарбӣ чунин навъҳои киберҷиноятҳо, аз қабили қаллобии компютерӣ (дар замони муосир қаллобӣ дар интернет) ва тамаъҷӯии компютерӣ (дар шароити рушди босруъати ТИК тамаъҷӯӣ дар фазои маҷозӣ бо таҳдиди ифшои маълумотҳои бадномкунанда), ба истилоҳ ҳифзи таҳмилӣ аз системаҳои компютерӣ ривоҷ ёфта дар қаламрави собиқ Иттиҳоди

Шуравӣ, солҳои 1979-1991 ва дар кишварҳои ғарб ИМА, охири солҳои 70-ум аввалин киберҷиноятҳо ба қайд гирифта шуда буд, ки аз ин навъи ҷиноят зарари бузурги моддиро аслан ташкилотҳои қарздиҳию молиявӣ дида буданд. Ҳамзамон дар ин марҳила аввалин таҳқиқоти вирусҳои компютерӣ, ки воситаи асосии содиршавии киберҷиноятҳо эътироф мегардад, анҷом дода шуда, аввалин барномаҳои зиддивирусиро таҳия намудаанд.

Ба ақидаи муаллифи рисола марҳилаи дуюми таҳаввулоти «вирусҳои компютерӣ» ба миёнаҳои солҳои 1980 то соли 1992 рост меояд. Дар давраи мазкур вирусҳои компютерӣ сохта мешаванд, ки барои кор дар компютерҳои дорои системаи амалиётии MS-DOS мутобиқ карда шудаанд. Паҳншавӣ ва зарари вируси мазкур тавассути фитаҳои (дискетҳо) иттилоотӣ-компютерӣ сурат мегирифт. Марҳилаи дуюми таҳаввулоти «вирусҳои компютерӣ» на танҳо боиси пайдоиш ва сабаби содир гардидани навъҳои нави киберҷиноятҳо балки асоси ташаккули ҷиноятҳое гардид, ки шабакаи интернетро ҳамчун воситаи содир намудани ҷиноят (барномаҳои зараровар ва ҳамлаҳои DoS) эътироф мекарданд, ки онҳоро ҷиҳати иҷроиш ба кор андохта, ба ин васила захираҳои шабакавӣ тобеъи киберҷиноятқорон гардида таҳдид ба амнияти иттилоотиро даҳчанд менамояд.

Марҳилаи сеюми таҳаввулоти «вирусҳои компютерӣ» то андозае бо шабакаи ҷаҳонии иттилоотию коммуникатсионӣ, яъне Интернет, ки шабакаи умумииҷаҳонии насли нав ба шумор меравад, алоқаманд аст. Дар ҳамин давра вирусҳое пайдо шуданд, ки дар баробари фаъолияти муътадили компютерҳоро халалдор сохтан, ҳатто телефони мобилиро низ халалдор месозанд (масалан, Timofonica, аввалин вируси компютерие, ки ба телефонҳои мобилӣ зарар мерасонад, 6 июни соли 2000 кашф шуда буд).

Ин давраи таҳаввулоти «вирусҳои компютерӣ», бо проблемаҳои ҷаҳонишавии дастгоҳҳои компютерӣ тавсиф мешавад, ки ҳамасола ҷомеаи ҷаҳониро ба мушкилотҳои барзиёд рӯ ба рӯ менамояд.

Таҳлили марҳилаи сеюми таҳаввулоти «вирусҳои компютерӣ», имкон медиҳад, ки маълум намоем, вирусҳои компютериро ҷиноятқорон бевосита барои системаҳои нави амалиётӣ, замимаи смартфонҳо ва нармафзори махсусе, ки дар бозори компютер пайдо мешаванд, таҳия кардаанд. Таҳаввулоти вирусҳо ба садҳо ҳазор компютерҳо дар саросари ҷаҳон таъсир мерасонад ва хисороти он аллакай миллиардҳо долларро ташкил медиҳад.

Марҳилаи чоруми таҳаввулоти «вирусҳои компютерӣ», ба ақидаи муаллифи рисола тақрибан солҳои 2006-2007 оғоз ёфта, то имрӯз идома дорад. Дар ин давра теъдоди «вирусҳои компютерӣ» садҳо миллион ба ҳисоб мешавад. Онҳо аллакай дар тамоми штаммҳо, аз ҷумла ба фазои маҷозӣ партофта шудаанд. Дар ҳоле ки дар тӯли 15 сол (аз соли 1992 то 2007) лабораторияи Касперский тақрибан 2 миллион барномаи нави зараровар ва вирусҳои компютериро ошкор карда буд, дар соли 2008 аллакай 15 миллион ва дар соли 2009 шумораи барномаҳои зараровар ва вирусҳои компютерӣ дар коллексияи лабораторияи Касперский ба 33 миллион расид.

Дар зербоби дуюми ин боб – **«Мафҳуми киберҷиноятҳо»** ба риштаи таҳлил кашида шудааст. Сарфи назар аз бартариҳои зиёди ТИК-и муосир, онҳо шароити наверо фароҳам овардаанд, ки ба содир намудани ҷиноятҳо дар сатҳи миллӣ ва байналмилалӣ мусоидат менамоянд. Даромад аз содиршавии ҷиноятҳо бо востаи ТИК дар ҷаҳон, пас аз даромад, аз тиҷорати маводи мухаддир ва силоҳ дар ҷойи сеюм қарор дорад. Ин ба пайдоиши як намуди нави фаъолияти ҷиноятӣ, аз қабили киберҷиноятҳо, ки дар марҳалаи ҳозира ба сатҳи хеле баланд расидааст, имконияти мусоид фароҳам меорад. Мавриди ба зикри хос аст, ки мафҳуми ҳуқуқии «киберҷиноятҳо» бори аввал соли 1978 дар қонунгузории ИМА муқаррар карда шудааст, ки мазмуни зеринро дошт, «дастрасии ғайриқонунӣ ба маълумот оид ба ҳаёти шахсӣ тавассути барномаҳои махсуси компютерӣ». Ҳамзамон, бояд қайд намоем, ки таърифи аввалини «киберҷиноятҳо» соли 1983 дар Париж (Фаронса) аз ҷониби гурӯҳи коршиносони Созмони ҳамкориҳои иқтисодӣ ва рушди Созмони Милали Муттаҳид ба таври зайл дода шудааст: «киберҷиноятҳо, ҳама гуна амали ғайриқонунӣ, ғайриахлоқӣ ё беиҷозат барои таъсир расонидан ба коркарди автоматии додаҳо ва (ё) интиқоли маълумот мебошад». Мафҳуми аз ҷониби муҳақиқону коршиносони СММ овардашуда пас аз мафҳуме, ки дар қонунгузории ИМА (соли 1978) пешбини гардидааст, дуюмин таърифи ин ҷиноят ифода гардида, албатта пурра мафҳуми киберҷиноятҳоро иникос намекунад, зеро ин кирдори барои ҷамъият хавфнок на танҳо дастрасии ғайриқонунӣ ё ғайриқонуни ҷамъ кардани маълумот оид ба ҳаёти шахсӣ тавассути барномаҳои махсуси компютерӣ ё беиҷозат таъсир расонидан ба коркарди автоматии додаҳо ва (ё) интиқоли маълумотро фарогир мебошад, балки он тавассути воситаҳои гуногуни ТИК ва таҷиҳизотҳои ёрирасони онҳо содир шуда зарарҳои гуногуни моддию маънавӣ мерасонад. Бо вуҷуди шумораи зиёди ҷиноятҳо бо истифода аз ТИК, дар қонунгузории Тоҷикистон мафҳуми «киберҷиноятҳо» вуҷуд надорад, ки ин ҳолат барои баҳои дурусти ҳуқуқи додан барои ин кирдор, муайян намудани сабабу шароитҳои содиршавии ҷинояти мазкур, пешбини намудани унсурҳои таркибии он ва мушахасу пурра намудани қонунгузории ҷиноятӣ имконият фароҳам намеорад. Ҳолати мазкур на танҳо барои таҳияи чораҳои ҳуқуқӣ оиди муқовимат ба ин навъи ҷиноят дар сатҳи миллӣ, балки барои ҷамъоварии маълумоти муқоисашавандаи оморӣ, рушди системаи ягонаи баҳисобгирӣ, дар сатҳи ҷаҳонӣ хеле муҳим аст.

Диссертант иброз менамояд, ки дар адабиётҳои илмӣ истилоҳи «киберҷиноятҳо» ҳоло дар баробари истилоҳи «ҷиноятҳои компютерӣ» истифода мешавад ва аксар вақт ин мафҳумҳо ҳамчун синоним истифода мешаванд. Аммо таҳқиқотҳои дар ин самт анҷомдодашуда, омӯзиши қонунгузории ҷиноятии давлатҳои пасошӯравӣ ва кишварҳои хориҷӣ дар ин самт маълум менамояд, ки ин истилоҳот синоними «киберҷиноятҳо» ифода намегардад. Мафҳуми «киберҷиноятҳо», нисбатан васеътар буда, ҳам бо истифодаи компютерҳо ва ҳам бо истифодаи ТИК ва шабакаи ҷаҳонии Интер-

нет содир мешаванд. Дар воқеъ, таҳлили истилоҳот нишон медиҳад, ки мафҳуми киберҷиноятҳо аз ҷиҳати мазмун, моҳият ва воситаи содиршавӣ, барои ҷамъият хавфнокӣ, гунаҳгорона ва зидди ҳуқуқи, нисбат ба ҳама мафҳумҳое, ки дар адабиёти илмӣ нисбати ин мафҳум синоним истифода мегардад, васеътар аст. Агар барои муайян кардани ҷиноятҳо муқобили амнияти иттилооти содир кардани амалҳои алоҳида нисбати ҳар як компютер, ҳатто онҳо ба ягон шабака пайваст нашуда бошанд, нигаронида шуда бошад, пас киберҷиноятҳо ҳатман таъсиреро дар назар дорад, ки тавассути ТИК ба дастгоҳҳои дурдаст амалӣ карда мешавад. Фарқияти дигар, дар он ифода меёбад, ки намудҳои ҷиноятҳо муқобили амнияти иттилоотӣ ҳамаҷониба ва мушахас дар боби алоҳида қонунгузорӣ пешбини гардидаанд, аммо кибеҷиноятҳо метавонанд ҳар гуна ҷиноятҳои пешбининамудаи қонунгузории ҷиноятӣ бошад.

Барои илми ҳуқуқшиносӣ дар айни замон таҳияи системаи махсус ва ё мафҳумҳое, ки тавсифи дақиқи киберҷиноятҳоро аз нуқтаи назари тарзи содир намудан ва тасниф намудани ин кирдорро таъмин мекунанд, зарур аст. Зеро ин кирдори барои ҷамъият хавфнок ҳамчун мушкилоти ҷиддии тамоми ҷомеаи ҷаҳонии муосир бо сатҳи баланди латентӣ ҳам ба иқтисоди миллӣ ва ҳам ба амнияти ҷаҳонӣ зарари бузурги моддию маънавӣ мерасонад ва метавонад дар фазои маҷозӣ тавассути истифодаи ТИК содир карда шавад.

Муаллиф қайд менамояд, ки барои таърифи мукаммали ин мафҳуми ҳуқуқӣ дар соҳаи технологияҳои иттилоотӣ корбурди ҷузъи калимаи «кибер», бамаврид аст. Истилоҳи «ҷиноятҳои компютерӣ» вобаста ба мазмуну моҳияти худ фарогирии тамоми ҷиноятҳои ин соҳа буда наметавонад. Мафҳуми «киберҷиноят» (англисӣ – cybercrime) нисбат ба мафҳуми «ҷиноятҳои компютерӣ» хеле васеътар аст, зеро он метавонад дар фазои иттилоотӣ ва ТИК моҳияти ҷиноятро хеле дақиқ ва пурратар муайян кунад.

Муҳаққиқ дар асоси таҳлили андешаҳои зикргардида ва таҳқиқи адабиётҳои соҳавӣ мафҳуми киберҷиноятҳоро, ки маҷмуи ҷиноятҳоро дар соҳаи шабакаҳои иттилоотӣ ва телекоммуникатсионӣ ифода менамояд чунин пешниҳод менамояд: «киберҷиноятҳо»- маҷмуи ҷиноятҳое, ки бо истифода аз воситаҳои барномавӣ–техникӣ ва ТИК дар фазои маҷозӣ бо мақсади ғайриқонунӣ ба даст овардан, тағйир додани иттилоот, несту нобуд ё бекор кардани системаҳо ва захираҳои иттилоотӣ нигаронидашуда, ҷиҳати расонидани зарар ба ҳуқуқу озодиҳои конститутсионии инсон ва шаҳрванд, амнияти давлатӣ ва ҷамъиятӣ ё муносибатҳои молу мулкӣ равона карда шудаанд.

Дар зербоби сеюми таҳқиқоти диссертатсионӣ – **«Таснифи киберҷиноятҳо»** таҳлил гардидааст.

Дар зербоби мазкур муаллиф бо дарназардошти тамоюли кунунии афзоиши компютеркунонӣ ва вобастагии бештари аҳолӣ аз Интернет инчунин тадричан бо суръати баланд паҳн шудани киберҷиноятҳо дар шакҳои гуногун, зарурияти таснифи киберҷиноятҳоро зарур шуморидааст. Зеро таснифи кирдорҳои ба ҷамъият хавфнок, ки қонунгузории ҷиноятӣ пешбинӣ намуда-

аст, аҳаммияти махсуси ҳуқуқӣ доранд, онҳо аломати ҳатмии мустаҳкамнамоии меъёрҳои қонунгузории ҷиноятӣ буда, барои банду басти ҷиноят, таъини ҷазо ё муайян намудани тарзи содиршавии ҷиноят таъсир мерасонанд, ки таснифи киберҷиноятҳо аз аҳамият дур нест.

Баъзе олимон таснифи киберҷиноятҳоро аз рӯйи истифодаи ТИК баррасӣ мекунанд. Дигарон бошанд вобаста ба объекти таҷовуз, аз рӯи низоми кори компютерҳо ва шабакаҳои интернетӣ (аз руи усулҳои содиршвай) ва аз руи хусусияти истифодабарии шабакаҳои компютерӣ таҳлил ва баррасӣ намудаанд

Рисоланавис дар зербоби мазкур таснифоти тамоми киберҷиноятҳоро аз рӯйи асосҳои зерин тасниф намудааст:

а) вобаста ба объекти таҷовузи ҷиноятӣ;

б) аз рӯйи хусусияти зараре, ки ба иттилооти компютерӣ расонида шудааст;

в) вобаста низоми киберҷиноятҳо;

г) вобаста ба усулҳои содир намудани ҷиноят;

Диссертант қайд менамояд, ки вобаста ба объекти таҷовузи ҷиноятӣ, киберҷиноятҳоро чунин тасниф намудан мувофиқи мақсад мебошад:

а) таҷовуз ба ҳуқуқ ва манфиатҳои соҳибони иттилооти компютерӣ. Ин гурӯҳ метавонад ҳарду амали барои ҷамъият хавфнокро дар м.298-и КҶ ҶТ (дастрасии ғайриқонунӣ ба иттилооти компютерӣ) ва м. 303-и КҶ ҶТ (таҳия, истифода ва паҳн намудани барномаҳои зараровар), ҳамзамон «қаллобии компютерӣ», «тахрибкории компютерӣ», «ҷосусии компютерӣ»;

б) таҷовуз ба ҳуқуқ ва манфиатҳои соҳибони воситаҳои иттилоот. Ба онҳо кирдорҳои барои ҷамъият хавфнок, ки дар қ. 3 м. 146 КҶ ҶТ пешбинӣ шудаанд, дохил шуда метавонанд (ғайриқонунӣ истеҳсол кардан, ба соҳибияти каси дигар додан ё соҳиб шудан бо мақсади ба соҳибияти каси дигар додани воситаҳои махсуси техникӣ, ки барои ниҳонӣ ба даст овардани маълумот), м. 304 КҶ ҶТ (вайрон кардани қоидаҳои истифодаи система ё шабакаи компютерӣ), «истифодаи беиҷозати барномаҳои компютерии муҳофизатшаванда», «истифодаи беиҷозати компютерҳо»).

Илова бар ин, қонунгузор расонидани зарарро вобаста ба шакли гуноҳ тафовут мекунад. Дар он аз як тараф қасдан несту нобуд кардан, маҳдуд кардан, тағйир додан ё нусхабардории иттилооти компютерӣ (м.м. 298-304-и КҶ ҶТ) ва аз ҷониби дигар, ҷавобгарӣ барои аз беэҳтиётӣ расонидан ин намуди зарар (қ. 2 м. 298, м. 299, м. 300, м. 303 ва қ. 3 м. 304 КҶ ҶТ) фарқ карда мешаванд.

Дар ин замина, диссертант иброз менамояд, ки вобаста ба низом, киберҷиноятҳоро метавон чунин тасниф намуд:

1. Ҷиноятҳо муқобили шабакаҳои интернетӣ ва таҷҳизотҳои ёрирасони онҳо (киберҷиноятҳои харобиовар):

Ҷиноятҳо муқобили шабакаҳои интернетӣ ва таҷҳизотҳои ёрирасони онҳо, аз осеб дидани додаҳо ва вайрон кардани тамомияти маълумот ва ам-

нияти кори системаҳои компютерӣ иборат аст. Чунин ҷиноятҳо инчунин метавонанд зарари молӣ расонанд.

2. Ҷиноятҳое, ки бо истифодаи шабакаи интернет ва захираҳои электронии иттилоотӣ (шабакаҳои иҷтимоӣ мессенҷерҳо ва дигар захираҳо) содир мегарданд. Кодекси ҷиноятии ҶТ дар 15 модда (моддаҳои 137, 137 (1), 144, 179 (1), 179 (3), 189, 241, 241 (1), 241 (2), 307, 307 (1), 307 (3), 373, 330, 334 (1) ва 396), ҷиноятҳоре, ки бо истифодаи шабакаи интернет содир мешаванд пешбинӣ намудааст. Ба ҷиноятҳои дигар, ки бо истифодаи шабакаи интернет содир мешаванд, инҳоро мансуб донистан мумкин аст: ба худкушӣ расонидан (м. 109 КҶ ҶТ), қаллобӣ (м. 247 КҶ ҶТ), муомилоти ғайриқонунии воситаҳои воситаҳои нашъадор (м. 200 КҶ ҶТ) ва тамаъҷӯӣ (м. 250 КҶ ҶТ), вале дар диспозитсияи ин моддаҳо ба таври махсус ҳолатҳои истифодаи шабакаи интернет зикр нагардидаанд.

3. Ҷиноятҳое, ки бо истифодаи воситаҳои гуногуни техникӣ содир мешаванд:

- Мактуби фишингӣ;
- Кибертаъқиб;
- Дуздии онлайнии маълумоти шахсӣ.

4. Ҷиноятҳое, ки ҳайё ва саломатиро дучори хатар мегузоранд.

- Таҳдиди зӯроварии ҷисмонӣ;
- Кибертаъқиб.

5. Ҷиноятҳое, ки махфияти иттилоотро вайрон мекунанд аз ҷумла дастрасии ғайриқонунӣ ба компютерҳо ё системаҳои компютерӣ бидуни расонидани зарар ба иттилоот.

Боби дуюми таҳқиқоти диссертатсионӣ – **«Масъалаҳои ҳуқуқӣ-ҷиноятии муқовимат бо киберҷиноятҳо дар сатҳи байналмилалӣ»** ном дошта, аз се зербоб иборат мебошад.

Дар зербоби якуми он – «**Ҳамкории байналмилалӣ дар муқовимат бо киберҷиноятҳо»** муаллиф қайд менамояд, ки таҷрибаи ҷаҳонӣ нишон медиҳад, ки киберҷиноятҳо ба зуҳуроти фаромиллӣ мубаддал гашта, ба ҷомеа ва амниятӣ ҳамаи давлатҳо таъсири манфӣ мерасонад, аз ин рӯ муқовимат бо киберҷиноятҳо ҳамкориҳои бевоситаи байналмилалиро талаб менамояд. Ҳамкориҳои байналмилалӣ, созмонҳои байналмилалӣ, ҷомеаи шаҳрвандӣ, бахшҳои хусусӣ ва коршиносон, самарабахш гардида, он ҳамчун усули муассири самарабахши муқовимат бо киберҷиноятҳо дар сатҳи байналмилаӣ ба ҳисоб меравад, зеро афзоиши таъсири технологияҳои иттилоотӣ, шабакаҳои иҷтимоӣ ва интернет ба ҳаёти муосири инсон, бисёр барномаҳои муфиду осонкунандаи муошират, паёмрасонҳои фаврӣ ва дигар намудҳои муошират пайдо шуданд.

Муаллиф таъкид менамояд, ки солҳои охир заминаи меъёрии ҳуқуқӣ ва ҳамкории давлатҳо дар самти муқовимат бо киберҷиноятҳо дар сатҳи байналмилалӣ, байниҳукуматӣ ва байниидоравӣ, фаъолона инкишоф меёбад. Дар баробари ин, дар миқёси ҷаҳонӣ то ҳол механизми ягонаи ҳуқуқии

ҷиноятӣ муқовимат бо киберҷиноятҳо дар сатҳи байналмилалӣ вуҷуд надошта, дар ин самт истилоҳоти ягона таҳия нашудааст, ки ин омил, ҳамкории давлатҳоро дар ин самт мушкил месозад.

Муҳаққиқ қайд мекунад, ки таҳлили Конвенсияи Иттиҳоди Аврупо оид ба киберҷиноят, ки ҳамкориҳои байналмилалиро дар муқовимат ба киберҷиноятҳо пешбинӣ менамояд, як механизми шаффофи ҳамкории байналмилалии давлатҳо ва мақомоти ҳифзи ҳуқуқи кишварҳои аъзои Конвенсияи зидди киберҷиноятҳо буда, хусусияти минтақавӣ дорад. . Аммо бояд гуфт, ки равиши минтақавӣ ба муттаҳидсозӣ ва ҳамоҳангсозии қонунгузории ҷиноятӣ дар доираи як гурӯҳи кишварҳо боиси парокандагии ҳамкории байналмилалӣ дар муқовимат ба киберҷиноятҳо мегардад ва имкон намедиҳад, ки ҳамкориҳои байналмилалиро байни мақомоти ҳифзи ҳуқуқи тамоми давлатҳо пурра таъмин карда шавад.

Диссертант иброз менамояд, ки ҳамкории давлатҳоро дар самти муқовимат бо киберҷиноятҳо метавон дар асосӣ санадҳои меъёрии ҳуқуқии байналмилалӣ (дар доираи созмонҳои бонуфузи байналмилалӣ аз ҷумлаи СММ, ИДМ, СПАД, СҲШ) ва санадҳои меъёрии ҳуқуқии байнидавлатӣ (шартнома, созишнома ва дигар санадҳои дуҷониба ва бисёрҷонибаи баимзорасидаи байни давлатҳо дохил мешаванд) тасниф намуд, зеро чунин шаклҳои ҳамкорӣ дар самти муқовимат бо киберҷиноятҳо, шакли муосир ва натиҷабахши ҳамкорӣ эътироф гардида, ҷиҳати татбиқи вазифаҳои дарназдошон гузошташуда, ичунин барои ҳарчизудтар барои ба ҳадафҳо ноил гардидан мусоид мебошад. Агарчанде ки бисёр кишварҳо қонунгузориҳои ҷиноятии худро ба қонунгузориҳои байналмилалӣ мутобиқ карда бошанд ҳам, алҳол қонуни ягонае вуҷуд надорад, ки мушкилоти ҳуқуқии ҷиноятӣ ва ҳамкории давлатҳоро дар ин самт ба таври зарурӣ аз байн барад. Дар ҷаҳони муосир танзими муносибатҳои ҳуқуқӣ дар такмили қонунгузориҳои сатҳи байналмилалӣ ва миллӣ шароити мусоид ба вуҷуд оварда, дар ин замина масъалаҳои баҳсталаб дар таркиби ҷиноятҳои алоҳида, аз ҷумла киберҷиноятҳо, ҳалли худро ба таври зарурӣ хоҳанд ёфт. Аз ин рӯ, вобаста ба моҳияти фаромиллӣ ва доираи киберҷиноятккорӣ, мавҷудияти далелҳои рақамии фаромиллӣ ҳамкории давлатҳоро дар самти муқовимат бо киберҷиноятҳо муаллиф ба гурӯҳҳои зерин ҷудо намудааст: ҳамкории миллии муқовимат бо киберҷиноятҳо; ҳамкории минтақавӣ; ҳамкории байналмилалӣ (ҳамкории байнидавлатӣ, байниҳукуматӣ ва байниидоравӣ).

Ҳамин тавр, ҳамкории байналмилалӣ дар муқовимат бо киберҷиноятҳо дар ин зербоб чунин тасниф гардидааст:

– ҳамкории байналмилалӣ дар муқовимат бо киберҷиноятҳо ҷиҳати эътирофи санадҳои универсиалӣ, минтақавӣ ва байнидавлатӣ (Конвенсияи Иттиҳодияи Аврупо оид ба киберҷиноятҳо соли 2001 (шаҳри Будапешт), Хартияи Окинава, «Созишнома дар бораи таъмини воситаҳои рақамӣ ва амнияти иттилоотӣ», «Созишнома дар бораи ҳамкорӣ байни кишварҳои

аъзои Иттиҳоди Давлатҳои Мустақил дар самти муқовимат бо ҷиноятҳои компютерӣ», «Созишномаи СҲШ оид ба таъмини амнияти байналмилалии иттилоотӣ», Созишнома оид ба табодули иттилоот дар соҳаи муқовимат бо ҷиноятҳо (Қарори сарони давлатҳои ИДМ аз 22 майи соли 2009, ш. Остона), Созишнома дар бораи ҳамкории кишварҳои аъзои ИДМ, дар мубориза бар зидди ҷиноятҳо дар соҳаи технологияҳои (Қарори СҲШ аз 28 сентябри соли 2018, ш. Душанбе), Барномаи ҳамкории кишварҳои аъзои ИДМ оиди мубориза бар зидди ҷиноятҳое, ки бо истифода аз технологияҳои иттилоотӣ содир мешаванд, барои солҳои 2016-2020 ва Созишнома байни Ҳукумати Ҷумҳурии Тоҷикистон ва Ҳукумати Туркманистон оид ба муҳамкорӣ дар соҳаи таъмини амнияти киберии байналмилалӣ ва Созишнома байни Ҳукумати Ҷумҳурии Тоҷикистон ва Ҳукумати Туркманистон оид ба ҳамкорӣ дар соҳаи ҳифзи техникии иттилоот аз 29 августи соли 2023, таҳти №381).

– ташкилотҳои байналмилалиро дар муқовимат бо киберҷиноятҳо ба намудҳои зерин ҷудо намудан мумкин аст:

1. Ташкилотҳои байналмилӣ: а) Созмони Миллали Муттаҳид; б) Интерпол – ташкилоти байналмилаии полиси ҷиноятӣ; в) Европол; г) Шурои Аврупо.

2. Ташкилотҳои минтақавӣ: а) СҲШ ва б) СПАД.

Ҳамаи ин ташкилотҳо дар ҳамоҳангсозии кӯшишҳои байналмилалӣ, бунёди ҳамкориҳои байналмилалӣ дар муқовимат бо киберҷиноятҳо нақши муҳим доранд.

Дар зербоби дуюми боби дуюми таҳқиқоти диссертатсионӣ **«Ҷавобгарӣ барои киберҷиноятҳо тибқи қонунгузории ҷиноятии кишварҳои хориҷӣ ва давлатҳои пасошӯравӣ»** диссертант зикр менамояд, ки проблемаи муқовимат бо киберҷиноятҳо, ки тавассути ТИК содир мешаванд таваҷҷуҳи давлатҳои ҷаҳонро ба худ ҷалб намудааст. Барои ҳалли он ҳам чорабиниҳои таъсиррасонии сиёсӣ-ҳуқуқӣ ва ҳам воситаҳои таъсиррасонии технологӣ истифода мегардад. Бояд қайд намуд, ки масъалаҳои таъмини амнияти иттилоотӣ, технологияҳои компютерӣ ва ҳифзи онҳо аз ҳамлаҳои киберӣ, аз ҷумла тавассути қонунгузории ҷиноятӣ ба танзим даровардани ин самти ҳаётан муҳим, имрӯз дар аксари кишварҳои пешрафтаи ҷаҳон аз масъалаҳои мубрам ба ҳисоб меравад. Қонунгузории ҷиноятии мамлакатҳои гуногун бо хусусиятҳои сиёсӣ, иқтисодӣ, идеологӣ, динӣ, фалсафӣ, сарчашмаҳо ва сохти меъёрҳои ҳуқуқ, инчунин дигар омилҳои хусусияти онҳоро муайянкунанда асос ёфтаанд. Таҳлили муқоисавии қонунгузории ҷиноятии давлатҳои хориҷӣ ва давлатҳои пасошуравӣ барои ошкор кардани рушди умумӣ ва махсуси меъёрҳое, ки ҷавобгариро барои содир кардани чунин ҷиноят пешбинӣ мекунанд, мусоидат менамоянд.

Аз ин лиҳоз, ҷавобгарии ҷиноятӣ дар самти киберҷиноятҳо дар низоми ҳуқуқи ҷиноятии кишварҳои пасошӯравӣ шакли ягонаро доро набудани муқовимат бо киберҷиноятҳо ва доираи амалҳои ғайриқонунӣ дар самти

киберҷиноятҳоро дар бар намегиранд. Вобаста ба ҷавобгарии ҷиноятӣ ҳангоми содир шудани киберҷиноятҳо метавон давлатҳои пасошӯравӣ ва давлатҳои хориҷиро шартан ба ду гурӯҳ метавон тақсим кард:

– давлатҳое, ки дар қонунгузории ҷиноятии онҳо меъёри махсуси ҷавобгарӣ барои содир намудани киберҷиноятҳо пешбинӣ шудаанд;

– давлатҳое, ки дар марҳилаи қабули қонунҳои дахлдор вобаста ба пурзӯр намудани ҷавобгарии ҷиноятӣ дар самти киберҷиноятҳо қарор доранд.

Дар асоси таҳлили ҷавобгарӣ ҷинояти барои содир намудани киберҷиноятҳо тибқи қонунгузории ҷиноятии давлатҳои давлатҳои хориҷ ва пасошуравӣ, ки ба оилаҳои гуногуни ҳуқуқӣ мансубанд, муаллиф аз нуқтаи назари танзими ҷавобгарӣ барои содир намудани киберҷиноятҳо чунин хулосабарори намудааст.

Ба мақсад мувофиқ аст, ки барои ҳифзи амнияти иттилооти аз ҳамлаҳои киберӣ қонунгузориҳои кишварҳои алоҳидаро ба таври дақиқ омӯхта, дар асоси онҳо қонунгузории ватаниро дар ин самт ба танзим даровард. Асри XXI ниёз ба пешрафти технологӣ дорад. Ҳазорон амалиёт аз ҷониби як ширкати технологӣ дар як лаҳза амалӣ мегардад, ки дар сурати танзими ҳуқуқӣ надоштани он ба одамон ва ба манфиати давлат, ҷомеа зарари зиёди молу мулкӣ расонида мешавад. Барои пешбини намудани меъёрҳои мушшахас барои киберҷиноятҳо ва пешгирӣ аз ин амали номатлуб бояд чораҳои амалиро дар сатҳи қонунгузорӣ роҳандозӣ намоем.

Дар баъзе давлатҳои дигар вобаста ба ҷавобгарии ҷиноятӣ татбиқи преюдитсияи маъмурӣ ҷой дорад. Яъне асоси танзими ҳуқуқии ин кирдорҳоро на танҳо қонунгузории ҷиноятӣ балки қонунгузории соҳаи ҳуқуқвайронкунии маъмурӣ низ пешбинӣ менамояд. (дар Қонунгузории ҷиноятии Австрия амалҳои номатлуб дар бахши ТИК ҷиноят шумурда намешавад, аммо ҷавобгарии маъмурӣ барои баъзе намудҳои ҳуқуқвайронкуниҳо дар «Қонун дар бораи дахлнопазирии маълумот», ки соли 2000 қабул шудааст, пешбинӣ мегардад).

Таҳлили муқоисавии намудҳои ҷазоҳои бо маҳрум сохтан аз озодӣ алоқаманд набуда ва ҷазоҳои бо маҳрум сохтан аз озодӣ алоқаманд, барои киберҷиноятҳо дар кодексҳои ҷиноятии давлатҳои посошӯравӣ ва кишварҳои хориҷӣ имконият медиҳад, хулоса намоем, ки онҳо аз ҳамдигар фарқ мекунанд. Миқдори нисбатан зиёди ҷазо дар КҶ Озарбойҷон ва КҶ Фаронса омадааст, ки инҳо – ҷарима, ва маҳрум кардани озодӣ мебошанд. Баръакс, ду намуди ҷазо дар КҶ Белгия (ҷарима ва маҳрум сохтан аз озодӣ), КҶ Италия ва Туркманистон (ҷазои маҳрум сохтан аз озодӣ ба муҳлати то 3 сол пешбинӣ шудааст) Узбекистон, Қазоқистон, Қирғизистон, Беларус ва Украина (ҷарима, маҳрум сохтан аз озодӣ) пешбинӣ карда шудаанд.

Дар қонунгузории ҷиноятии кишварҳои хориҷӣ, унсурҳои таркибии киберҷиноятҳо дар фаслҳои (бобҳои) гуногуни Кодекси ҷиноятӣ ҷойгир шудаанд.

Кодекси ҷиноятии ҶТ ҷавобгарии ҷиноятиро танҳо нисбати шахси воқеӣ ҳамчун субъекти ин ҷиноят эътироф мекунад, аммо дар системаҳои ҳуқуқи ҷиноятии оилаҳои ҳуқуқии Скандинавия ва дар баъзе кишварҳои низоми оилаи ҳуқуқии Романо-Олмонӣ, шахси ҳуқуқӣ низ метавонад ҳамчун субъекти ҷиноят баромад кунад. Вале баъзе давлатҳо, ба монанди Италия доираи ҷавобгарии ҷиноятиро бо нишон додани дигар шахсон – шахси мансабдор, васеъ кардаанд.

Дар баъзе давлатҳои хориҷӣ ҷавобгарӣ барои дуздӣ, ки тавассути истифодаи технологияҳои иттилоотӣ–коммуникатсионӣ содир шудааст ва қаллоби дар интернет дар меъёрҳои махсуси ҳуқуқии ҷиноятӣ ҷавобгариро пешбини менамояд – қаллобӣ (дар Русия, Молдова) ё оид ба ҷиноятҳои хусусияти қаллобидошта (дар Британияи Кабир, Австралия, ИМА) ифодаи худро меёбад.

Дар зербоби сеюми боби дуюм **«Тафриқагузории ҷавобгарии ҷиноятӣ барои киберҷиноятҳо тибқи қонунгузории ҷиноятии кишварҳои хориҷӣ»** мавриди омӯзиш қарор гирифта, рисоланавис кӯшиш намудааст, ки қонунгузории ҷиноятии давлатҳои хориҷро вобаста ба ҷавобгарии ҷиноятӣ барои киберҷиноятҳо ба риштаи таҳлил кашида хулосаҳои илмии судманд пешниҳод намояд. Муаллиф нуқтаи назари гуногунро таҳлил намуда, ба хулосае омадааст, ки тафриқагузории ҷавобгарии ҷиноятӣ роҳи асосии рушди қонунгузории ҷиноятӣ ва сиёсати ҳуқуқӣ–ҷиноятии Ҷумҳурии Тоҷикистон дар ҳалли вазифаи назариявӣ ва амалии ҳуқуқии ҷиноятӣ, мутобиқ намудани механизми ҳифзи ҳуқуқ ба шароити ҷомеаи иттилоотӣ мебошад. Доктринаи ҳуқуқии ҷиноятӣ бо мавҷудияти як қатор таҳқиқотҳои фундаменталӣ оид ба моҳият, намуд, восита ва меъёрҳои тафриқабандии ҷавобгарии ҷиноятӣ арзёбӣ карда мешавад. Аз таҳлили андешаҳои олимон ва таҳқиқи адабиёти илмӣ диссертант иброз менамояд, ки тафриқагузории ҷавобгарии ҷиноятӣ бояд аз рӯи тарзи содиршудани ҷиноят, субъекти ҷиноят, тарафи объективии ҷиноят ва аз рӯи моддаҳои алоҳидаи қонунгузории ҷиноятӣ ба роҳ монда шавад. Талошҳои қонунгузор барои тафриқагузории ҷавобгарии ҷиноятӣ, ба андешаи муҳақиқ, ба ноил шудан ба ҳадафи умумӣ ва ҳамзамон дурусту муносиб вобаста ба мушкилиҳову таҳдидҳои замонӣ муосир, инчунин таъмини ҳифзи ҳуқуқӣ-ҷиноятии манфиатҳои умум ва хатарҳои бузург нигаронида шудааст.

Дар асоси ин гуфтаҳо диссертант хулосагирӣ менамояд, ки дар қонунгузории кишварҳои хориҷӣ барои баррасии ин самти ҷиноятқорӣ иқдомҳои зиёде роҳандозӣ шудааст. Таҳлилҳои нишон медиҳад, ки намудҳои нави киберҷиноятҳо аз ҷумла: ғайриқонуни ба даст овардани иттилооти компютерӣ, вайрон намудани фаъолияти муътадили воситаҳои нигоҳдорӣ, коркард ё интиқоли иттилоот, чун қоида, дар боби ҷиноятҳо муқобили шахсият, моликият ё амнияти ҷамъиятӣ баррасӣ карда мешаванд.

Кишварҳои хориҷӣ бо муқаррар намудани тафриқагузорӣ дар ҷавобгарии ҷиноятӣ барои дахолат ба махфият, пуррагӣ ва дастрасии худи

иттилооти компютерӣ ва барои амалҳои ғайриқонунӣ нисбат ба воситаҳои нигоҳдорӣ, коркард ё интиқоли он (воситаҳои коркарди автоматикунонидашудаи маълумот) тавсиф мешаванд.

Баръакси қонунгузории кишварҳои хориҷӣ, муқовимат ба киберҷиноятҳо бо муқаррар кардани ҷавобгарии на танҳо барои таҳия, паҳн ва истифодаи барномаҳои зарарноки компютерӣ, балки барои амалҳои ғайриқонунии марбут ба таҷҳизот, ки барои содир кардани он маълум аст, инчунин таҳдид ба амнияти додаҳо ва системаҳо, барои паҳн кардани маълумот дар бораи идентификаторҳои шабака (воситаҳои иҷозатдиҳии корбар) роҳандозӣ карда мешавад.

Хусусиятҳои асосии вазнинкунандаи киберҷиноятҳо тибқи қонунгузории ҷиноятии кишварҳои хориҷӣ инҳоянд: 1) аз ҷониби гурӯҳӣ шахсон содир намудани ҷиноят; 2) содир намудани ҷиноят нисбат ба объектҳои инфрасохтори муҳимми иттилоотӣ; 3) фаро расидани оқибатҳои вазнин; 4) содир намудани ҷиноят бо истифодаи барномаҳои зарарноки компютерӣ ё воситаҳои гуногуни техникие, ки дидаю дониста барои таъсири ғайриқонунӣ ба иттилооти компютерӣ ё воситаҳои нигоҳдорӣ, коркард ё интиқоли он равона карда шудаанд.

Басо муҳим аст, ки барои бисёре аз киберҷиноятҳо дар кишварҳои хориҷӣ имкони ба зиммаи шахсони ҳуқуқӣ гузоштани ҷавобгарии ҷиноятӣ пешниҳод карда мешавад.

Дар баробари ин, хусусияти муҳимм дар қонунгузории давлатҳои хориҷӣ мавҷудияти он меъёрҳое мебошад, ки татбиқи муқаррароти анъанавии қонуни ҷиноятиро ба шаклҳои нави «рақамӣ»-и ҷиноят қонунӣ мегардонанд. Ҳамин тариқ, ин кишварҳо бидуни тағйир додани сохторҳои ҳуқуқии мавҷуда, ба назар чунин мерасанд, ки доираи амали худро ба таври қонунӣ васеъ мекунанд ва ба ин восита масъалаи бозгӯӣ намудани аломатҳои таркибҳои ин навъи ҷиноятҳои анъанавиро баррасӣ менамоянд.

Барои рафъи мушкилоти мавҷуда дар самти киберҷиноятҳо, ки дар даврони муосир падидаи нав мебошад, аз таҷрибаи ҳуқуқии давлатҳои пешрафта бояд истифода бурда, дар такмили қонунгузорӣ ҳолатҳои татбиқшавандаро дар амалияи ин навъи ҷиноят ба инобат гирем. Маҳз дар ҳамин зина, муқовимат бо ин навъи ҷиноятҳо самарабахш ҳисобида мешавад, ки тавассути он танзими муносибатҳои ҳуқуқӣ дар ҷомеаи мутамаддин амалӣ мегардад.

Ҳамин тавр, дар алоқамандӣ бо тафриқагузории ҷавобгарӣ барои киберҷиноятҳо тибқи қонунгузории ҷиноятии кишварҳои хориҷӣ, вобаста ба тарзи содиршавии киберҷиноятҳо давлатҳоро ба 2 гурӯҳ тақсим кардан мумкин аст.

Ба гурӯҳи аввал давлатҳое ворид карда мешаванд, ки барои аз ҷониби провайдерон ичро нагардидани қарорҳои субъектони муборизабаранда бо киберҷиноятҳо оид ба бастани захираҳои интернетии дахлдор ва нест кардани маълумоти манъшуда, мусоидати маҷозӣ (виртуалӣ) барои содир намуда-

ни киберҷиноятҳо, истифодаи захираҳои интернетӣ бо мақсади паҳн кардани маълумот дар бораи усулҳои содир намудани ҷиноят (масалан моддаҳои моддаи 285А, 286А, 287А, 287В Кодекси ҷиноятии Чин) ҷавобгарии ҷиноятиро пешбини менамояд. Аммо бархе аз кишварҳо кирдорҳои дар моддаи 285А-и Кодекси ҷиноятии Чин пешбинишуда на ҷавобгарии ҷиноятӣ балки ҷавобгарии маъмуриро муқарар намудааст (масалан моддаи 13.34 Кодекси ҳуқуқвайронкунии маъмурии Федератсияи Русия).

Ба гурӯҳи дуюм давлатҳое ворид карда мешаванд, ки барои ҷиноятҳое, ки бо истифода аз ТИК содир мешаванд, аз ҷумла қаллобии интернетӣ ҷавобгарии ҷиноятиро муқарар намудаанд. Масалан, Кодекси ҷиноятии Ҷумҳурии Молдова (моддаи 260 (5)), Кодекси ҷиноятии Федератсияи Россия (моддаи 159.6), Қонуни Британияи Кабир оид ба қаллобӣ (England fraud act 2006), Кодекси ҷиноятии Испания (моддаи 248) Кодекси ҷиноятии Белгия (моддаи 147), Кодекси ҷиноятии Дания (моддаи 279(а)), Кодекси ҷиноятии Эстония (§ 213).

Боби сеюм **«Тавсифи ҳуқуқӣ-ҷиноятии ҷиноятҳо ба муқобили шабакаҳои интернетӣ ва таҷҳизотҳои ёрирасони онҳо»** аз се зербоб иборат аст.

Зербоби якуми боби сеюм **«Объекти ҷиноятҳо ба муқобили шабакаҳои интернетӣ ва таҷҳизотҳои ёрирасони онҳо (барномаҳои зараровар, ҳамлаҳои DoS)»** ном дошта, дар он аз нигоҳи илми ҳуқуқи ҷиноятӣ таҳлили объект ҷиноят ба роҳ монда шудааст.

Дар рисола зикр карда шудааст, ки проблемаи объекти ҷиноят нисбат ба проблемаи гуноҳ ва расонидани зарар камаҳаммият набуда, балки аз лиҳози фалсафӣ проблемаи амиқтар мебошад, вале он дар адабиёти ҳуқуқӣ кам таҳқиқу коркард гардидааст. Аммо айни замон объекти ҷиноятҳо ба муқобили шабакаҳои интернетӣ ва таҷҳизотҳои ёрирасони онҳо бо далели истифодаи технологияҳои компютерӣ ва иттилоотию коммуникатсионӣ дар содир намудани навъҳои зиёди кирдорҳои барои ҷамъият хавфнок ба истилоҳ «анъанавӣ» гуногун арзёбӣ мегардад. Зеро ҷаҳони муосирро бе пешрафти технологӣ тасаввур кардан ғайриимкон буда, тамоми корбарони технологияҳои муосири иттилоотию коммуникатсионӣ дар фаъолияти худ як маротибае бо таъсири манфӣ – барномаҳои зараровари компютерӣ ва ҳамлаҳои DOS рӯ ба рӯ мешаванд. Ин навъ барномаҳои зараррасонро якранг наметавон тасниф намуд: қисме аз онҳо нисбатан безараранд, қисми дигар метавонанд на танҳо ба дороиҳои иттилоотӣ, балки ба худи таҷҳизоти компютерӣ зарари ҷуброннопазир расонанд. Муаллиф қайд менамояд, ки проблемаҳои объекти ҷиноятҳо муқобили шабакаҳои интернетӣ ва таҷҳизотҳои ёрирасони онҳо, аз ҷумла барномаи зараровар ва ҳамлаҳои DoS, дар айни замон хеле баҳсталаб ифода гардида вобаста, ба масъалаи мазкур аз шумораи умумии таҳқиқотҳои анҷомёфта ҳамагӣ 2%-и пажуҳишҳо ба ин самт равона гардидаанд, ки дар шароити бо суръат инкишоф ёфтани технологияҳои иттилооти-коммуникатсионӣ воқеан ҳам нигаронкунанда

арзёбӣ мегардад.Дар асоси таҳлили ҳамаҷонибаи адабиёти илмӣ диссертант иброз менамояд, ки объекти умумии ин ҷиноятҳоро муносибатҳои ҷамъиятӣ ва амнияти ҷамъиятӣ фаро мегирад. Аз ин лиҳоз, муносибатҳои ҷамъиятие, ки баронмаҳои зараровар ва ҳамлаҳои DoS ба онҳо зарар мерасонанд, барои ҷомеа махсусан муҳиманд, ҳимояи онҳо бояд бо чораҳои муассиртарин ва самарабахш амалӣ карда шавад.

Масъалаи дигареро, ки рисоланавис дар зербоби мазкур мавриди таҳлил қарор додааст, ин объекти намудии ҷиноятҳо ба муқобили шабакаҳои интернетӣ ва таҷҳизотҳои ёрирасони онҳо мебошад. Муҳаққиқ иброз менамояд, ки дар марҳилаи муосири рушди илми ҳуқуқи ҷиноятӣ нуқтаи назари дигарро дар масъалаи объекти намудии ҷиноят низ дидан мумкин аст. Ҷиҳати муайян кардани навъи объекти намудии ҷиноятҳо ба муқобили шабакаҳои интернетӣ ва таҷҳизотҳои ёрирасони онҳо андешаҳои муҳаққиқон бо ҳам мувофиқат надорад. Ҷиноятҳо муқобили шабакаҳои интернетӣ ва таҷҳизотҳои ёрирасони онҳо (барномаҳои зараровар, ҳамлаҳои DoS) мазмунан дар боби 28 КҶ ҶТ «Ҷиноятҳо ба муқобили амнияти иттилоотӣ» мустаҳкам шудаанд. Аз ин лиҳоз диссертант ба хулоса меояд, ки объекти намудии ҷиноятҳо муқобили шабакаҳои интернетӣ ва таҷҳизотҳои ёрирасони онҳо, муносибатҳои муҳими ҷамъиятии бо қонунгузории ҷиноятӣ ҳифзшаванда дар соҳаи бехатарии таҳия, истифода ва паҳнкунии иттилооти компютерӣ, захираҳои иттилоотӣ, системаҳои иттилоотӣ ва ТИК, яъне ҳуқуқ ва манфиатҳои шахсонӣ воқеӣ ва ҳуқуқӣ, ҷамъият ва давлат оид ба истифодаи системаи автоматикии коркарди маълумот ташкил медиҳад.

Муаллиф қайд менамояд, ки яке аз меъёрҳои таснифоти ҷиноятҳо муқобили шабакаҳои интернетӣ ва таҷҳизотҳои ёрирасони онҳо (барномаҳои зараровар, ҳамлаҳои DoS) дар боби 28-и Кодекси ҷиноятии Ҷумҳурии Тоҷикистон объекти бевоситаи ҷиноят мебошад, ки маҷмуи муносибатҳои ҷамъиятиро аз нигоҳи истифодаи қонунӣ ва бехатари иттилооти компютерӣ ва захираҳои иттилоотӣ дар бар мегирад. Объекти бевоситаи ҷиноятҳо муқобили шабакаҳои интернетӣ ва таҷҳизотҳои ёрирасони онҳо муносибатҳои зерини ҷамъиятиро фаро мегирад, ки онро чунин тасниф менамоем: 1) дастрасии қонунӣ, сохтан, коркард, табдил додан ва истифодаи иттилооти компютериро таъмин менамояд; 2) фаъолияти бонизоми МЭҲ ва ё шабакаи онҳо; 3) манфиатҳои соҳибкорӣ, ки ба муомилоти таҷҳизоти ин компютерҳо алоқаманд мебошанд. Объекти бевоситаи ин ҷиноят, ки аз беэҳтиётӣ боиси оқибатҳои вазнин гардидааст, дар асоси қисми 2-и моддаи 303-и Кодекси ҷиноятӣ – муносибатҳои ҷамъиятӣ, ки вобаста ба хусусияти онҳо дигар арзишҳои аз ҷиҳати иҷтимоӣ муҳимро (ҳаёти инсон, саломатии одамон ва ғ.) таъмин мекунанд, баррасӣ мешавад. Объекти иловагии ин ҷиноятҳо муносибатҳои ҷамъиятие мебошанд, ки бо меъёрҳои ҳуқуқ танзим шуда, ҳуқуқ ва манфиатҳои қонунии шахс, ҷомеа ва давлатро таъмин мекунанд.

Аз баррасӣ ва таҳлили объекти ҷиноятҳо муқобили шабакаҳои интнренети ва таҷҳизотҳои ёрирасони онҳо диссертант ба хулосае омад, ки ин кирдорҳои барои ҷамъият хавнок (баронмаҳои зарароват, ҳамлаҳои DoS) на танҳо ба амнияти иттилоотӣ зарар мерасонад, балки ба муносибаҳои гуногуни ҷамъиятӣ ва ё гурӯҳи калони номуайяни одамон (мисол, дар ҳолати кибертерроризм) зарар мерасонанд ё таҳдиди расонидани чунин зарарро ба миён меоранд. Қонунгузории ҷиноятии ватанӣ категорияи ҷинояти мазкурро дар боби 28 «Ҷиноятҳо ба муқобили амнияти иттилоотӣ» пешбинӣ намудааст, ва бо дарназардошти дигар муносибатҳои ҷамъиятиро дар бар гирифтани ин боб (кибертерроризм, киберэкстремизм, кибертаъқиб, мактуби фишигӣ) мувофиқи мақсад мешуморем, фасли нав дар КҶ ҶТ бо номи «Ҷиноятҳо муқобили амнияти киберӣ» ворид карда шавад.

Рисоланавис иброз менамояд, ки корбурди объекти иловагӣ хусуситяи ихтиёрӣ дорад. Мавҷудияти он ба ҳифзи ҳуқуқ ва манфиатҳои қонунии шахс, ҷомеа ва давлат нигаронида шудааст. Объекти иловагӣ метавонад, масалан, молу мулк, ҳуқуқи муаллиф, ҳуқуқ ба дахлнопазирӣ, сирри шахсӣ ва оилавӣ, амнияти экологӣ, асосҳои сохти конститутсионии Ҷумҳурии Тоҷикистон ва ғайра бошанд. Мавҷудияти объекти иловагӣ, албатта, дараҷаи барои ҷамъият хавфнокии ҷиноятро баланд мебардорад, ки ҳангоми ба гунаҳгор таъин кардани ҷазои одилона бояд ба назар гирифта шавад. Объекти иловагии ин ҷиноятҳо муносибатҳои ҷамъиятие мебошанд, ки бо меъёрҳои ҳуқуқ танзим шуда, ҳуқуқ ва манфиатҳои қонунии шахс, ҷомеа ва давлатро таъмин мекунанд.

Зербоби дуюми боби сеюм **«Тарафи объективии ҷиноятҳо ба муқобили шабакаҳои интернетӣ ва таҷҳизотҳои ёрирасони онҳо (барномаҳои зарароват, ҳамлаҳои DoS)»** ном дошта, дар он аломатҳои тарафи объективии ҷиноятҳо ба муқобили шабакаҳои интернетӣ ва таҷҳизотҳои ёрирасони онҳо мавриди таҳқиқот қарор гирифтааст.

Муаллиф қайд мекунад, ки муқаррар намудани аломатҳои тарафи объективии ин ҷиноятҳо барои бандубасти кирдорҳоии мазкур ва минбаъд ба ҷавобгарӣ кашидани шахси онро содиркарда аҳаммияти муҳим дорад.

Диссертант қайд менамояд, ки аломатҳои тарафи объективии ҷинояти мушаххас дар диспозитсияи моддаҳои қисми махсуси КҶ ҶТ инъикос меёбанд. Агар дар диспозитсияи меъёр нишондиҳандаи мавҷудияти оқибатҳои барои ҷомъият хавфнок вуҷуд надошта бошад, пас ин таркиби ҷиноят расмӣ аст. Ҳамин тариқ, ҷиноят аз лаҳзаи содир шудани кирдори барои ҷамъият хавфнок хотимаёфта ҳисобида мешавад. Аз ин рӯ, тарафи объективии ҷиноят дорои аломатҳои мушаххасе мебошанд, ки онҳоро ба ду гурӯҳ ҷудо мекунанд: аввалан, аломатҳои ҳатмӣ-(кирдори барои ҷамъият хавфнок (ҳаракат ё беҳаракатӣ), оқибати кирдор ва робитаи сабабӣ), дуюм, аломатҳои иловагӣ. Тарафи объективии ҷиноятҳо ба муқобили шабакаҳои интернетӣ ва таҷҳизотҳои ёрирасони онҳоро муносибатҳои ҷамъиятие, ки дар натиҷи содиршавиашон ба иттилооти дар компютер мавҷудбуда ё сис-

темаи компютерӣ, интернет ва таҷҳизотҳои ёрирасони онҳо зарар меоранд, ифода мегардад. (модем, wifl, роутер, антенаҳои махсус, моҳвора, таҷҳизоти мобилӣ) (ки воситаи содиршаваии ҷиноятҳои баррасишаванда, ба монанди кирмҳои шабакавӣ, вирусҳои файлии классикӣ, троянҳо, воситаҳои хакерӣ ва дигар барномаҳоро дар бар мегиранд). Муҳаққиқ аз руи таҳқиқоти анҷомёфта тарафи объективии ҷиноятҳо ба муқобили шабакаҳои интернетӣ ва таҷҳизотҳои ёрирасони онҳо (барномаҳои зараровар, ҳамлаҳои DoS)-ро дар ҳаракатҳои зерин пешбини менамояд: таҳияи барномаҳои зараровари компютерӣ бо мақсади бе иҷозат нобуд ё муҳосира кардан ё тағйир додан ё нусхабардории иттилоот, ки дар системаи ё шабакаи компютерӣ ё дар махзани мошинҳо маҳфуз аст; даровардани тағйир дар барномаҳои вуҷуддошта бо мақсади бе иҷозат нобуд ё муҳосира кардан ё тағйир додан ё нусхабардории иттилоот, ки дар системаи ё шабакаи компютерӣ ё дар махзани мошинҳо маҳфуз аст; таҳияи барномаҳои махсуси вирусдор (ҳамчун намуди барномаҳои зараровар); паҳн намудани махзанҳои дорои барномаҳои махсуси вирусдор; аз кор баровардани дастгоҳи компютерӣ; вайронкунии шабакаҳои компютерӣ; ҳамлаҳое, ки барои қатъи шабакаҳои алоқа ва роутерҳо нигаронида шудаанд (моҳияти ин ҳамла фиристодани ҷараёни бузурги бо ном флудӣ ба компютери ҳамлашуда, яъне дархостҳои нодуруст ё моҳиятан бемаънӣ мебошад. Ин омил тамоми шабакаҳои додаҳо ё роутери вурудро комилан маҳкам мекунад. Азбаски ҳаҷми маълумот аз ҳаҷми захираҳои коркард зиёд аст, гирифтани бастаҳои дурусти додаҳо аз корбарони дигар ғайриимкон мегардад. Дар натиҷа, система аз хидматгузорӣ бозмемонад, ҳамлаҳое, ки ба пурсозии системаи операторсионӣ ё захираҳои барнома нигаронида шудаанд (ин навъи ҳамлаҳо на ба шабакаи алоқа, балки ба худи система нигаронида шудаанд. Ҳар як система дорои маҳдудиятҳои зиёд оид ба ғунҷоишҳои гуногун (вақти протсессор, фазои диск, хотира ва ғайра) мебошад ва мақсади чунин ҳамла равонасозии система барои вайрон кардани ин маҳдудиятҳо мебошад. Барои ин ба компютери шахси ҷабрдида шумораи зиёди дархостҳо фиристода мешаванд. Дар натиҷаи ин амал сервер, система аз хидматрасонии дархостҳои корбарони қонунӣ бозмемонад).

Муаллиф иброз менамояд, ки дар нақши аломатҳои факултативии тарафи объективи тарз, олот, восита, ҷой, вақт ва шароит (вазъият) содиршавии ҷиноят баромад мекунанд. Дар ҳолатҳое, ки аломатҳои мазкурро меъёри ҳуқуқи ҷиноятӣ пешбинӣ менамояд, онҳо ҳамчун аломати ҳатмии таркиби ҷинояти мушаххас баромад мекунанд.

Воситаи содиркунии ҷиноят ин предметҳое мебошанд, ки барои осон гардонидани содиркунии ҷиноят истифода мегарданд, масалан воситаи содиршавии ҷиноятҳо ба муқобили шабакаҳои интернетӣ ва таҷҳизотҳои ёрирасони онҳо, кирмҳои шабакавӣ, вирусҳои файлии классикӣ (яке аз намудҳои барномаҳои зараровар), троянҳо, воситаҳои хакерӣ, барномаи ҷосусӣ ва барномаҳои тамаъҷӯӣ ва рамзшиканӣ, ташкил менамояд.

Дар зербоби сеюми боби сеюм **«Аломатҳои субъективии ҷиноятҳо ба муқобили шабакаҳои интернетӣ ва таҷҳизотҳои ёрирасони онҳо (барномаҳои зараровар, ҳамлаҳои DoS)»** мавриди таҳқиқоти илмӣ қарор гирифтааст. Муаллиф қайд мекунад, ки ҷиноят ҳамчун кирдори барои ҷамъият хавфнок дар натиҷаи бо ҳам мавҷуд будании ҳамаи аломатҳои таркибии ҷиноят нишонаҳои объективӣ ва субъективӣ содир мешавад. Умумияти ин нишонаҳо дар он ифода мегарданд, ки онҳо воқеияти ҷиноятро ба таври гуногун баҳо медиҳанд. Барои истифодаи дурусти меъёрҳои қонунгузории ҷиноятӣ таҳлили муфассали ҳамаи аломати таркиби ҷиноят аҳамияти муҳим дорад. Муҳаққиқ иброз менамояд, ки оид ба масъалаи субъекти ҷиноятҳо ба муқобили шабакаҳои интернетӣ ва таҷҳизотҳои ёрирасони онҳо (барномаҳои зараровар, ҳамлаҳои DoS) дар илми ҳуқуқи ҷиноятӣ фикру ақидаҳо зиёд буда, мавқеи ягонаву мушаххас ҷой надорад. Баъзе олимон зарурати муқаррар намудани синни ҷавобгарии ҷиноятиро барои содир намудани ҷиноятҳое, ки ба муқобили шабакаҳои интернетӣ ва таҷҳизотҳои ёрирасони онҳо (барномаҳои зараровар, ҳамлаҳои DoS) нигаронида шудааст, аз 14-солагӣ асоснок мешуморанд, муҳаққиқони дигар қатъиян ба ин тадбир мухолифанд.

Ба андешаи диссертант субъекти ҷиноятҳо ба муқобили шабакаҳои интернетӣ ва таҷҳизотҳои ёрирасони онҳо метавон шахси воқеии мукаллафи ба синни 14-сола расида бошад, зеро дар ин синну сол шахс аҳамияти иттилооти компютерӣ, шабакаҳои компютерӣ ва ТИК-ро дарк мекунад ва қоидаву усулҳои истифодаи онҳоро медонад. Муҳимтар аз ҳама, дар шароити ҷаҳонишавӣ ва дастрасии технологияҳои гуногуни иттилооти-коммуникатсионӣ ба шахсони ҳанӯз ба синни 14-солагӣ нарасида зиёд ба мушоҳида расида, онҳо аз хатари иҷтимоии вайрон кардани қоидаҳои истифодаи технологияҳои кибернетикӣ, аз ҷумла иттилооти компютерӣ, огоҳ ҳастанд.

Аз баррасии субъекти ҷинояти мазкур, муҳаққиқ иброз менамояд, ки барои ҷиноятҳое, ки ба муқобили шабакаҳои интернетӣ ва таҷҳизотҳои ёрирасони онҳо (барномаҳои зараровар, ҳамлаҳои DoS) нигаронида шудаанд, метавонад дилхоҳ шахси воқеӣ ва мукаллаф бошад (яъне субъекти умумии ҷиноят), ки дар вақти содир кардани ҷиноят ба синни 14 расидааст. Зарур мешуморем, ки ба қисми 2-и моддаи 23-и Кодекси ҷиноятии Ҷумҳурии Тоҷикистон (оид ба синну соли ҷавобгарии ҷиноятӣ) бо таркиби ҷиноятҳое, ки дар моддаҳои 300 ва 303-и Кодекси ҷиноятии Ҷумҳурии Тоҷикистон пешбинӣ шудаанд, илова ворид карда шавад ва ҷавобгарии ҷиноятӣ барои ин гуна ҷиноятҳо аз синни 14-солагӣ муқаррар карда шавад. Ба андешаи муаллиф, поён фаровардани синни ҷавобгарии ҷиноятӣ барои шахсони воқеии синнашон ба 14 расида комилан қобили қабул аст, аммо ин раванд танҳо дар ҳолатҳое, ки ба муқобили шабакаҳои интернетӣ ва таҷҳизотҳои ёрирасони онҳо (барномаҳои зараровар, ҳамлаҳои DoS) оқибатҳои вазнин дошта бошад ё хатари сар задани онҳоро ба миён оварда бошад. (масалан, барои содир на-

мудани таркиби ҷиноятҳои таснифшудаи моддаи 300 ва моддаи 303-и Кодекси ҷиноятии Ҷумҳурии Тоҷикистон) қобили қабул мебошад. Барои асоснок намудани ин нуқтаи назар метавон ба таҷрибаи як қатор кишварҳои хориҷа, (қонунгузории ҷиноятии Франсия, Шветсия, Латвия, Дания) ки дар онҳо ҷавобгарии ҷиноятӣ барои содир намудани ҷиноятҳое, ки ба муқобили шабакаҳои интернетӣ ва таҷҳизотҳои ёрирасони онҳо (барномаҳои зараровар, ҳамлаҳои DoS) нигаронида шудааст аз синни 14 ё 15-солагӣ муқаррар карда мешавад, бояд такя намуд. Ҳамзамон чунин синну соли пасти ҷавобгарӣ барои ҷиноятҳои дар боло номбаршуда аз он иборат аст ки: 1) моҳияти иҷтимоии чунин кирдорҳо аз тарафи шахсони синни 14 ё 15-солагӣ хуб дарк карда мешавад; 2) чунин кирдорҳо хусусияти баланди хавфнокии ҷамъиятӣ доранд; 3) ин ҷиноятҳо дар байни шахсони синни 14 ё 15-солагӣ васеъ паҳн шудаанд.

Муаллиф қайд менамояд, ки ҷаҳонишавӣ, рушди босуръати технологияҳои иттилооти коммуникатсионӣ ва оқибатҳои зарароварӣ онро ҳоло аксари кишварҳои пешрафтаи ҷаҳон эътироф намуда дар қонунгузории ҷиноятии худ субъекти ҷиноятҳо ба муқобили шабакаҳои интернетӣ ва таҷҳизотҳои ёрирасони онҳо (барномаҳои зараровар, ҳамлаҳои DoS)-ро, «шахсони ҳуқуқи» пешбини менамоянд.

Муаллифи рисола зикр менамояд, ки мавҷудияти аломатҳои амалҳои барқасдона тибқи таҳқиқотҳои анҷомдодашуда дар мавриди таҳияи барномаи зараровар ва ҳамлаҳои DoS баррасии ҳамаҷонибаро талаб менамояд. Аз ин лиҳоз мавҷудияти зарарнокии барнома тасдиқи қасди бевоситаи содир кардани ҷиноят мебошад. Тарафи субъективии ҷиноятҳо ба муқобили шабакаҳои интернетӣ ва таҷҳизотҳои ёрирасони онҳо танҳо бо қасди бевоситаи киберҷинояткор дар алоқа бо дарки барои ҷамъият хавфнокии кирдори ӯ тавсиф карда мешавад, зеро ки ӯ имконият ё ногузирии фаро расидани оқибати барои ҷамъият хавфноки онро пешбинӣ намуда, хоҳони фаро расидани он бошад.

Боби чорум **«Тавсифи ҳуқуқии ҷиноятии ҷиноятҳои бо истифода аз воситаҳои гуногуни техникӣ содиршаванда»** аз се зербоб иборат аст. Зербоби якум ба **«Объекти ҷиноятҳое, ки бо истифода аз воситаҳои гуногуни техникӣ содир мешаванд (мактуби фишингӣ, кибертаъқиб, дуздии онлайнии маълумоти шахсӣ)»** бахшида шудааст.

Ба ақидаи муаллиф барои бандубасти дилхоҳ ҷиноят таҳлили ҳуқуқӣ-ҷиноятии унсурҳои таркиби ҷиноят талаб карда мешавад. Таркиби ҷиноят яке аз институтҳои марказии ҳуқуқи ҷиноятӣ ба шумор меравад. Асоси ҷавобгарии ҷиноятӣ, хусусан киберҷиноятҳоро кирдоре ташкил медиҳад, ки дар он тамоми аломатҳои таркиби ҷиноятҳо ҷой дошта бошад(м. 11 КҶ ҶТ). Яке аз аломатҳои таркиби ҷиноят, ки барои бандубаст аҳамият дорад, ин объекти ҷиноят мебошад. Объекти ҷиноят дар таҳлили ҳама гуна меъёри қисми махсуси Кодекси ҷиноятӣ ҳамчун унсури таркиби ҷиноят, хусусан киберҷиноятҳо дар ҷои аввал гузошта мешавад. Зеро, дуруст муқаррар кар-

дани объекти ҷиноят ба мо имкон медиҳад, ки моҳияти иҷтимоии ин ҷиноятҳоро дарк намуда, мавқеи онро дар байни дигар муносибатҳо ва муносибатҳои ҷамъиятӣ, ки дар ҷомеа инкишоф меёбанд, инчунин барои дарачаи ба ҷамъият хавфнокии манфиатҳои бо қонуни ҷинояти ҳифзшавандаро муайян намоем. Аз ин рӯ диссертант дар натиҷаи таҳлили адабиётҳои соҳавӣ ба хулосае, меояд, ки тибқи он ба сифати объекти ҷиноятҳои бо истифода аз воситаҳои гуногуни техникӣ содиршаванда метавонад ҳам муносибатҳои ҷамъиятӣ (масалан, дар соҳаи мубодилаи амнияти иттилооти компютерӣ) ва ҳам шахс, манфиатҳои гуногуни шахсӣ ва иҷтимоӣ (ҳаёт, саломатӣ, мукотибот, андеша ва мулоҳизаҳои шахсӣ ва дигар арзишҳои моддӣ ва ғайримоддӣ), инчунин ҳуқуқ ва манфиатҳои шахсони воқеӣ ва ҳуқуқӣ, муносибатҳои ҳуқуқӣ, ки аз ҷониби қонун ҳифз карда мешаванд (яъне, шахсони воқеӣ ва ҳуқуқӣ) баромад намоянд.

Рисоланавис дар робита ба он, ки боби 28 КҶ ҶТ «Ҷиноятҳо ба муқобили амнияти иттилоотӣ» пешбини гардидааст, пешниҳод менамояд, ки объекти хелии ин ҷиноятҳоро амнияти иттилоотӣ ташкил менамояд.

Объекти намудии ҷиноятҳое, ки бо истифода аз воситаҳои гуногуни техникӣ содир мешаванд маҷмуи муносибатҳои ҷамъиятие мебошад, ки ҳолати амнияти шахсият, ҷомеа ва давлатро аз таҳдидҳои дохилию берунии кибернӣ дар шакли нигоҳдорӣ, интиқол ва дигар истифодабарии иттилооте таъмин месозад, ки аз ҳисоби он татбиқи ҳуқуқ ва озодиҳои конститутсионии инсон ва шаҳрванд, инчунин истиқлолияти миллӣ, тақсимнопазирии ҳудудӣ ва рушди устувори иқтисодию иҷтимоии ҶТ, мудофиа ва амнияти давлат таъмин карда мешавад.

Объекти бевоситаи кирдорҳои баррасишаванда инҳо баромад карда метавонанд: шаъну шараф, эътибор ва обрӯи шахс; ҳуқуқи ҳар шахс ба дахолатнопазирии ҳаёти шахсӣ, сирри шахсӣ ва оилавӣ; ҳуқуқи инсон ва шаҳрванд ба дахлнопазирии мукотиба, суҳбатҳои телефонӣ, мактубҳои почтавӣ, телеграфӣ; ҳуқуқҳои муаллифӣ ва ҳуқуқҳои ба он алоқаманди инсон ва шаҳрванд; муносибатҳои молумулкии ҷамъиятӣ; муносибатҳои ҷамъиятии таъминкунандаи ҳифзи иттилооти тиҷоратӣ, андозӣ ё бонкӣ аз дастрасии ғайриқонунӣ ба он. Муаллиф ин андешаро бо асоснок менамоем, ки ҷиноятҳое, ки бо истифода аз воситаҳои гуногуни техникӣ содир мешаванд (мактуби фишингӣ, кибертаъқиб, дуздии онлайнии маълумоти шахсӣ) моҳияташ дар он ифода мегардад, ки киберҷинояткорон тавассути интернет эълонҳои бардуруғро ҳамарӯза дар шабакаҳои иҷтимоӣ дар гардиш қарор дода бо роҳи фиреб ба боварии шаҳрвандон даромада ҳуқуқ ба молу мулк, маълумотҳои шахсӣ, тавассути фиристонидани паёмак, ки гӯё шаҳрванд дар лотерея бурд намудааст ё ин ки дастгирии молиявӣ ва иштирок дар лоиҳаҳои сармоягузории ширактҳои қаллобии хориҷӣ, пешниҳоди кӯмакҳои молиявӣ аз ҷониби сиёсатмадорон ва шахсони саховатманд, мерос мондани маблағ аз ким кадом як хеши дур, пешниҳод намудани туҳфаҳо аз хориҷӣ кишвар дар намуди «баста (посилка)» ва монанди

инҳоро паҳн намуда, бо роҳи фиреб барои тасарруфи маблағҳои шаҳрвандон ташкил ва роҳандози менамоянд.

Зербоби дуюми боби чорум ба **«Тарафи объективии ҷиноятҳое, ки бо истифода аз воситаҳои гуногуни техникӣ содир мешаванд (мактуби фишингӣ, кибертаъқиб, дуздии онлайнии маълумоти шахсӣ)»** бахшида шудааст. Муҳақиқ, қайд менамояд, ки дар баробари дигар аломатҳои таркиби ҷиноят, тарафи объективии ҷиноят барои муқаррар кардани таркиби ҷинояти мазкур мавқеи муҳимро ишғол менамояд. Маълум аст, ки тарафи объективии ҷиноят муносибати зоҳирии кирдори барои ҷамъият хавфноке мебошад, ки ба объекти бо қонуни ҷиноятӣ ҳифзшаванда таҷовуз карда ба он заррар мерасонад. Он аз маҷмуи аломатҳое иборат аст, ки ҷониби берунаи кирдори барои ҷамъият хавфнокро тавсиф медиҳад. Ин унсури таркиби ҷиноят дорои аломатҳои ҳатмӣ ва факултативӣ мебошад.

Диссертант дар натиҷаи таҳлили андешаҳои олимон хулоса менамояд, ки тарафи объективии ҷиноятҳое, ки тавассути воситаҳои гуногуни техникӣ содир мешаванд ин маҷмуи аломатҳоеро дар бар мегирад, ки муносибатҳои зоҳирии шахсро вобаста ба ҷамъоварии ғайриқонунии маълумот дар бораи шахси дигар, паҳн кардани маълумот дар доираи васеъ, ба таври оммавӣ ва ё дар воситаҳои ахбори омма намоиш додани маълумот, инчунин ирсоли мактубҳо бо роҳи фиреб ҳангоми истифода аз шабакаи интернет, ки расонидани зарар ба ҳуқуқ ва манфиатҳои қонунии ҷабрдидаро ба вуҷуд меорад ташкил медиҳад.

Яке аз ин аломатҳо аломатҳои факултативии тарафаи объектии ҷиноятҳо ин ҷойи содир шудани ҷиноят мебошад. Бо сабаби он, ки ин ҷиноятҳо тавассути шабакаҳои интернетӣ содир мешаванд, ҷойи содир шудани ин ҷиноятҳо тамоман барои бандубасти онҳо аҳамият надоранд. Қонунгузории ҷиноятӣ низ вобаста ба ин масъала дар ягон меъёр бартарӣ надодааст. Аз ин лиҳоз баррасии ҷойи содир шудани ин ҷиноятҳо тамоман аҳамият надорад.

Дигар унсури таркибии факултативӣ ин тарзи содиршавии ҷиноят мебошад. Тарзи содир намудани ҷиноят ин маҷмуи усул ва тариқе ки гунаҳгор дар вақти содир намудани кирдори барои ҷамъият хавфнок истифода мебарад.

Аз муқарароти КҶ ҶТ бармеояд, ки тарафи объективии ҷиноят тарзи содир намудани ҷиноятро дар меъёрҳои моддаҳо ба таври мушаххаст нишон додааст. Масалан, КҶ ҶТ дар меъёрҳои боби ҷиноятҳо муқобили амнияти иттилоотӣ одатан чунин меъёрҳоро ба монанди «бо роҳи фиреб» «бо истифодаи интернет» «ғайриқонунӣ ворид шудан ба иттилооти компютерӣ» ва ғайраҳо муқаррар кардааст, ки онҳо ҳамчун тарзи содир намудани ҷиноятҳои мазкур (яъне тарафи объективии ҷиноят) эътироф карда мешавад.

Вобаста ба ин масъала муҳаққиқ ба назарияи илм ва таҳкими қонунгузории ҷиноятӣ рӯ овардааст. Тавре дар рисола зикр карда шудааст, мактуби фишингӣ, кибертаъқиб, дуздии онлайнии маълумоти шахсӣ масъа-

лаи баррасии мо мебошанд. Тарзи содир шудани ин ҷиноятҳоро дар алоҳидагӣ баррасӣ кардан мувофиқи мақсад аст, зеро тарзи содиршавии ин ҷиноятҳо бо ду роҳ сурат мегиранд: 1) ирсоли мактубҳо бо роҳи фиреб ва 2) содиршавии онҳо тавассути интернет.

Зербоби сеюми боби чорум ба таҳлили **«Аломатҳои субъективии ҷиноятҳое, ки бо истифода аз воситаҳои гуногуни техникӣ содир мешаванд (мактуби фишингӣ, кибертаъқиб, дуздии онлайнии маълумоти шахсӣ)»** равона гардидааст. Диссертант қайд менамояд, ки қонунгузории ҷиноятӣ ҷавобгариро барои киберҷиноятҳо, ки бо истифода аз воситаҳои гуногуни техникӣ содир мешаванд (мактуби фишингӣ, кибертаъқиб, дуздии онлайнии маълумоти шахсӣ) пешбинӣ накардааст, аммо рушди содиршавии ин ҷиноятҳо дар ҷомеаи ҷаҳонӣ рӯз то рӯз инкишоф меёбад. Муайян кардани аломатҳои субъективии ин ҷиноятҳо ҳангоми истифода аз воситаҳои гуногуни техникӣ барои содир намудани ҷиноят аҳаммияти муҳими назариявӣ ва амалӣ дорад. Аломати субъективии ҷиноятҳои мазкур мисли аломати субъективии ҷиноятҳо дар умум ду элементи таркибиро дар бар мегирад. Яъне тарафи субъективӣ ва субъекти ин ҷиноят.

Муаллиф зикр мекунад, ки тарафи субъективии ҷиноятҳои баррасишаванда шаклҳои гуногуни содиршавиеро доро мебошад, ки тарафи дохила (рӯҳии) таҷовузи киберҷинояткоронро тавсиф медиҳанд. Тарафи субъективӣ ин ҷиноятҳо дар шакли қасди бевосита содир гардида, бо нияти ба даст овардани молу мулк, ғайриқонунӣ ба даст овардани маълумоти шахсӣ, таъқиби шахс, бастани иттилоот ва нобудсозии он ифода мегардад, ки чун ҳадафи «ғаразнок» тавсиф мешавад. Мақсади ғаразноки содир кардани ин ҷиноятҳо қасдан ба шахси дигар расонидани зарари молумулкӣ ё ғайримолумулкӣ, ки ба ҳаёти шахсии шахс ва истифодаи ин маълумотҳо муқобили ӯ, инчунин дигар амалҳо (,анҷом додани қаллобии андоз ё суғуртаи тиббӣ аз номи ҷабрдида дастрасӣ ва ғ) мебошад.

Ба ақидаи муаллиф аломатҳои субъективии ҷиноятҳое, ки бо истифода аз воситаҳои гуногуни техникӣ содир мешаванд (мактуби фишингӣ, кибертаъқиб, дуздии онлайнии маълумоти шахсӣ) танҳо бо қасди бевосита тавсиф карда мешавад, ки пеш аз ҳама аз огоҳӣ оид ба, ғайриқонунӣ ба даст овардани иттилооте, ки дар системаи компютерӣ, шабакаи компютерӣ ва дар махзани мошинҳо мавҷуданд ва хоҳиши содир кардани ин кирдори барои ҷомеа хавфнок зоҳир мегардад. Дар таркибҳои бардубастшаванда, субъект аз усули содир кардани ҷиноят (истифодаи зӯроварӣ ё таҳдиди истифодаи он, тарсонидан, масхара, чалби таввачух, дарёфти маълумот, халалдор кардани амният ва идора кардани дигарон бо роҳи таҳдид зуроварӣ) огоҳ аст, мехоҳад маҳз бо ҳамин усулҳо ин кирдори барои ҷамъият хавфнокро содир намояд.

Субъекти ин ҷиноятҳо ҳам умумӣ ва ҳам махсус шуда метавонанд. Ин намуди ҷиноятҳоро метавонанд шахсоне содир кунанд, ки ТИК ва барномасозиро хуб медонанд ва бо фаъолияти умумии шабакаи интернетӣ шинос мебошанд. Маҳз ҳамин омил ба онҳо имкони содир намудани ин навъи

ҷиноятро фароҳам меорад. Дар эътирофи сукбъекти ин ҷиноятҳо муҳим он нест, ки шахс корманди ин ё он ташкилот ё муассиса бошад. Шаҳрвандони оддӣ низ ин ҷиноятҳоро содир карда метавонанд.

Дар баробари субъектони зикршуда операторон ва провайдерон низ субъектони ин ҷиноят эътироф шуда метавонанд. Зеро онҳо тавассути хизматрасониҳои алоқаи барқӣ паҳн ё таблиғ намудани ҳама гуна иттилоот бар зидди асосҳои сохтори конститутсионӣ, амнияти шахсӣ, ҷамъиятӣ, давлатӣ, иттилоот дар бораи маҳдуднамоии ҳуқуқу озодиҳои инсон ва шаҳрванд, барангехтани кинаю адовати динию мазҳабӣ ё низои миллӣ, нажодӣ, маҳалгарой, паст задани шаъну эътибори миллӣ, тарзи омодасозӣ ва тарғиби маводи нашъаовар, тарканда ва маводи дигари заҳролудкунанда, ба содир намудани ҷиноят ва ҳуқуқвайронкунии маъмурӣ равонагардида, хусусияти экстремистию террористидошта, порнография, аз ҷумла порнографияи кӯдакона, инчунин паҳн намудани ҳама гуна маълумот, ки бо санади судии эътибори қонунӣ пайдонамуда ва қонунгузории Ҷумҳурии Тоҷикистон манъ шудааст, содир карда метавонанд.

Боби панҷуми таҳқиқоти диссертатсионӣ – «**Таҳқиқи криминологии киберҷиноятҳо**» ном дошта, аз се зербоб иборат мебошад.

Дар зербоби якуми он – «Ҳолат, сохтор ва пастуболоравии (динамикаи) киберҷиноятҳо» бо хусусиятҳои назаррас ба риштаи таҳлил кашида шудааст. Рисоланавис бар он андеша аст, ки дар ҷомеаи муосир киберҷиноятқорӣ ба як падидаи муташаккил ва густурда табдил ёфта, танзими муносибатҳои иҷтимоӣ ба он вобастагии зиёд пайдо менамояд. Зеро ин омилҳои мураккабнизом ба дарёфти маълумотҳои зарурӣ вобаста ба ҳолат, сохтор ва динамика оид ба киберҷиноятҳо алоқамандӣ дорад.

Дар рисола пешбини карда шудааст, ки бештари ҷиноятҳои содиргардида дар самти киберҷиноятҳо дар соҳаи обу энергетика ва ширкатҳои мобилӣ бештар ба назар мерасад, ки зарарӣ расонидашуда дар ин соҳаҳо миллионҳо сомониро ташкил медиҳад. Аз тарафи кормандони Вазорати корҳои дохилии Ҷумҳурии Тоҷикистон дар давраи солҳои 2018-2020 аз 51 киберҷиноятҳои содиршуда танҳо 43-тоашро ошкор намудаанд, яъне он 84%-ро ташкил медиҳад. Ҳолати ошкор нагардидани чунин ҷинояҳо нигаронкунанда арзёбӣ шуда, он таҳдиди воқеӣ ба амнияти миллӣ ва иттилоотӣ мебошад. Ҷараёни мазкурро ҳатто давлатҳои аъзои ИДМ низ сипарӣ намуда истодаанд, чунончи соли 2020 дар ИДМ ҳиссаи парвандаҳои ҷиноияи бо ҳукми айбдоркунӣ ба суд ирсолшуда 18,2% (2018 – 24,8%, 2019 – 23%) аз шумораи умумии ҷиноятҳои ба қайдгирифташуда дар ин самтро ташкилмедиҳад, ки 73,6%-и онҳо дар соли 2020 ошкор нашуданд (2018 – 66,5%, 2019 – 68,4%). Аз маълумотҳои овардашуда бармеояд, ки содиршавии барзиёди киберҷиноятҳо дар Федератсияи Россия, Ҷумҳурии Белоруссия ва Ҷумҳурии Озарбойҷон мушоҳида мегардад. Ҳамин тавр, омори содиршавии киберҷиноятҳо дар давлатҳои аъзои ИДМ нишон медиҳад, ки соли 2020 шумораи ҷиноятҳои бақайдгирифташуда, дар самти киберҷиноятҳо 4 маротиба

афзудааст, яъне аз 125 244 ҳолат дар соли 2018 то ба 536 516 ҳолат дар соли 2020 расидааст.

Муаллиф хулосаҳои худро дар диссертатсия оиди таҳқиқи криминологии киберҷиноятҳо ба шакли зерин пешниҳод менамоед:

– Содиршавии киберҷиноятҳо бо истифода аз ТИК дар айни замон рӯ ба афзоиш дорад. Аз ин лиҳоз зарур аст, ки барномаҳои таълимӣ ва стандартҳои давлатии дар самти мазкур қабул гардида аз нав дида баромада шуда, шумора ва сифати мутахассисони тайёркарда дар самти амнияти киберӣ зиёд карда, малакаи кормандони мавҷуда, ки дар ин самт фаъолият мекунанд, баланд бардошта шавад, инчунин бо ҷалби олимони соҳа, мутахассисони варзидаи техникӣ, собиқадорони соҳа, ташкили институти такмили ихтисоси соҳаи таъмини амнияти иттилооти аз ҳамлаҳои киберӣ танҳо ба манфиати кор аст, зеро таҳқиқотҳо нишон доданд, ки яке аз унсурҳои асосии таъмини амнияти иттилоотӣ аз аз ҳамлаҳои киберӣ ва пешгирии киберҷиноятҳо ин рушди иқтидори таълимӣ ва илмии кишвар мебошад.

– Омори расмии Сармаркази иттилоотӣ-таҳлилии Вазорати корҳои дохилии Ҷумҳурии Тоҷикистон ҳаҷми воқеӣ ва хусусияти ҳамлаҳои кибериро пурра инъикос намекунад.

– Киберҷиноятқорон дар самти истифодаи интернет, воситаҳои гуногуни техникӣ ва таҳияи барномаҳои зараровар дониши васеъ дошта, ҳадафҳои асосии фаъолияти ғайриқонунии онҳо хусусияти санҷиши дониши худро дорад. Аз ин рӯ, муборизаи бо киберҷиноятқорӣ бояд бо ҷалби мутахассисоне сурат гирад, ки ин хусусиятҳоро мавриди омӯзиш қарор дода бошад.

– Таҳдиди бузургтарин ба амнияти иттилооти компютерии ҳифзшуда аз ҷониби корбарони дохилии система мебошад. Вобаста ба ин, такмил додани дараҷаи касбии мутахассисон ва мониторинги эътимоднокии онҳо аз ҷониби хадамоти амнияти ширкат аҳаммияти хоса дорад.

– Надонистани қурбониёни киберҷиноятҳо аз воситаҳо ва усулҳои асосии ҳифзи иттилооти худ, ба ҳамлагар имкон медиҳад, ки ба осонӣ амалҳои ғайриқонунӣ содир кунад. Вобаста ба ин, инъикоси нақшаҳои маъмултарини киберҷиноятҳо ва роҳҳои пешгирӣ аз онҳо дар ВАО, инчунин дар байни аҳолӣ ташаккул додани малакаҳои коркарди иттилооти компютерӣ ва омӯзиши кор бо дастгоҳҳои гуногуни техники аз ҷумла интернет аҳаммияти муайян дорад.

– Аксари қурбониёни киберҷиноятҳо шахсони ҳуқуқӣ мебошанд. Вобаста ба ин, корхонаю ташкилотҳоро зарур аст, ки ба таъмини амнияти компютерӣ аз ҳамлаҳои киберӣ таваҷҷуҳи ҷиддӣ дода, дар нақшаи корӣ вазифаи мутахассиси ҳифзи иттилоотро муайян намуда, барои татбиқи он чорабиниҳои намояд.

– Дараҷаи баланди киберҷиноятҳо бештар ба душвории ошкор кардани кирдори киберҷиноятқор ва худдории ҷабрдида барои хабар додан ба мақомоти ҳифзи ҳуқуқ алоқамандӣ дорад.

Яке аз тамоюлҳои асосии рушди киберҷинояткорӣ саривақт ошкор накардани он мебошад. Раванди роҳандозии ғайриқонунии шабакаҳои иттилоотию коммуникатсионӣ, мессенҷерҳои фаврӣ ва интернет ба ин раванд мусоидат мекунанд. Истифодаи технологияи навин дар муомилоти молиявӣ ва қарзӣ, тиҷорати онлайнӣ, рамзгузории маълумот ва ғайра ба давлат ва ҷомеа имкон намедиҳад, ки шумораи зиёди киберҷиноятҳоро саривақт пешгирӣ кунанд, зеро онҳо бо сабабҳои технологӣ сарфи назар карда мешаванд.

Дар зербоби дуюми боби панҷум масъалаи «**Хусусиятҳои криминологии шахсияти киберҷинояткор**» мавриди таҳқиқ қарор гирифтааст. Диссертант, иброз менамояд, ки пешгирии бомуваффақияти ҷиноятҳо танҳо дар он ҳолат имконпазир аст, ки ба шахсияти ҷинояткор диққати махсус дода мешавад. Бинобар ин, қайд кардан зарур аст, ки чунин категория, ба монанди шахсияти ҷинояткор – унсури асосӣ ва муҳими ҳамаи механизми рафтори ҷиноятӣ ба шумор меравад. Хусусиятҳои хос, ки сабаби ба амал омадани рафтори ҷиноятӣ мегарданд, бояд объекти бевоситаи чораҳои пешгирикунанда ва огоҳкунанда гарданд. Бинобар ин, масъалаи шахсияти ҷинояткор ба шумораи пешоҳанг ва ҳамзамон ба яке аз масъалаҳои мубрам дохил мешавад. Масъалаи шахсияти ҷинояткор – яке аз масъалаҳои муҳими илми криминология, қисми таркибии мавзӯи илми мазкур ба шумор меравад. . Ин мафҳум барои киберҷинояткорӣ аҳаммияти махсус пайдо мекунад, зеро ки дар ошкор ва тафтиши ҷиноятҳо он унсури ниҳоят муҳим аст.

Ба ақидаи муаллиф ба гурӯҳҳо тасниф намудани ҷиноят вобаста ба амалҳои ҷинояткор, ки тавассути ТИК амалӣ мешавад, муҳим ба шумор меравад. Чор дараҷаи чунин қобилиятҳо вуҷуд дошта, ҳар яке аз ин гурӯҳҳо дорои хусусиятҳои хос аст.

Дараҷаи якум ба имкониятҳои ҳадди ақали гузаронидани муколама дар низоми худкор буда, онро тавассути ба кор андохтани барномаҳои мушаххас барои коркарди иттилоот амалӣ мекунанд.

Дараҷаи дуюм қобилияти таҳия ва оғоз кардани барномаҳои инфиродии коркарди иттилоотро дар шакли муосири технологӣ дар бар мегирад.

Дарҷаи сеюм имкон медиҳад, ки кори система назорат шуда, ба барномаи асосии он бевосита таъсир расонида шавад.

Дараҷаи чорум тамоми имкониятҳои шахсонеро, ки лоиҳакашӣ, татбиқ ва таъмири таҷҳизоти техникии ин низоми технологиро иҷро мекунанд, фарогир мебошад. Аз таҷриба бармеояд, ки киберҷинояткор мутахассиси баландихтисос буда, дар хусуси низоми технологӣ ва иттилоотӣ ҳама нозукиҳоро медонад.

Муаллиф дар асоси такя ба сарчашмаҳои муътамад оид ба паҳлуҳои гуногуни шахсияти киберҷинояткорон (парвандаи ҷиноятӣ, ҳисоботи расмии оморӣ, натиҷаҳои тадқиқоти криминологӣ) чунин шахсонро ба гурӯҳҳои зерин ҷудо намудааст:

1. Вобаста ба намуди киберҷинояткорӣ ва сатҳи малакаҳои кор бо системаҳои компютерӣ:

– шахсоне, ки дар ин самт маълумоти олӣ дошта, дар содир намудани киберҷиноятҳо соҳибтачриба буда дорои донишҳои махсус ба шумор мераванд. Мавҷудияти дониши махсус маънои онро дорад, ки чунин ҷиноятқор ба қатори хакерҳо (крекерҳо) мансуб аст;

– шахсоне, ки қаблан ҷиноят содир намуда, ба сифати киберҷинояткор «ба таври махсус тайёр шудаанд», онҳо фирефтаи имкониятҳои васеи фазои маҷозӣ, инчунин намояндагони ҷиноятҳои муташаккил гардидаанд, ки ин тоифа қодиранд одамони дорои дониши махсусро барои содир намудани ҷиноят муттаҳид намуда, кӯшишҳои асосии худро барои ба даст овардани фоида равона созанд.

2. Ҳолати пешгирии фаъолияти ҷинояткорона:

– фаъолияти асосии ҷинояткоронаи худро танҳо дар фазои маҷозӣ амалӣ месозанд. Ҳамзамон, агар он саривақт пешгирӣ карда шавад, рафтори чунин шахсон хатарнок ба таври назаррас зери назорат қарор мегирад;

– дар фазои маҷозӣ ва ҳаёти воқеӣ амалиёти ҷиноятӣ анҷом додан.

3. Вобаста ба сабабҳои кирдори ҷинояткорона:

– навъи тамаъкорона аз ҷониби шахсоне ташаккул меёбад, ки майли ошкори мусодираи манфиатҳои моддӣ ва дигар омилҳои муҳимро (ҷоизаҳои варзишӣ ва ғ.) тавассути содир намудани киберҷинояткорӣ доранд;

– навъи зӯроварӣ. Набудани робитаи ҷисмонӣ дар фазои маҷозӣ содир намудани ҷиноятҳо муқобили шахсиятро (таҳдид ба худкушӣ, таҳдиди кушшор) бо роҳи таъсири руҳӣ, кибертаъқиб, тарсондан, инчунин даъват ба ҳамлаҳои зӯроварӣ истисно намекунад;

– навъи номуташаккили иҷтимоӣ ё истилоҳи бо ном «бозӣ». Ҳадафи асосии киберҷинояткор вайрон кардани меъёрҳои иҷтимоӣ ва ҳуқуқӣ, расонидани таъсири харобиовар ба ҷомеа ва муносибатҳои ҷамъиятӣ мебошад;

– навъи эътироз. Киберҷиноят ҳамчун як шакли эътироз, роҳи муборизаи сиёсӣ ё идеологӣ;

– навъи худтанзимкунанда. Ҷинояткорон хоҳиши ба даст овардани мақоми баландтари иҷтимоии ғайрирасмиро дар ҷомеаи киберӣ доранд;

4. Вобаста ба хусусиятҳои равони киберҷиноятрон онҳоро ба гурӯҳҳои зерин метавон ҷудо кард:

– навъи шаҳватпарастӣ;

– навъи дорои хусусиятҳои идеологӣ ва сиёсӣ;

– навъи киберҷинояткор вобаста ҳолат;

– навъи таҳқиқотӣ;

Дар зербоби сеюми боби панҷум масъалаи «**Таҳлил, огоҳонидан ва пешгирии киберҷинояткорӣ**» мавриди таҳқиқи илмӣ қарор гирифтааст.

Диссертант қайд менамояд, ки яке аз вазифаҳои муҳимтарини мақомоти ҳифзи ҳуқуқ, ки дар даврони муосири ташаккули муносибатҳои нави бозорӣ умр ба сар мебаранд, танзими рушди ҷомеаи демократӣ вобаста

ба пешрафти босуръати технологияҳои иттилоотӣ буда, дар ин самт мубориза бо киберҷиноятҳо ва махсусан ба муқовимат ба таҳия, истифода ва паҳн кардани барномаҳои зараровар, ҳалаҳои DoS, кибертаъқиб, мактубҳои фишингӣ ва дуздии маълумоти шахсӣ, аҳаммияти аввалиндараҷаро касб менамояд. Муаллиф аҳаммияти мушкилоти киберҷиноятро дар ду ҳолат муайян кардааст.

Якум, афзоиши босуръати таҳия, татбиқ ва истифодаи технологияҳои нави иттилоотӣ. Сониян, истифодаи босуръати технологияҳои нав барои нойл шудан ба ҳадафҳои ғайриқонунӣ ва густариши технологияҳои инноватсионӣ, аз ҷумла технологияҳои иттилоотӣ дар муҳити ҷиноятӣ.

Аз ин рӯ, дар шароити муосир на танҳо технологияҳои иттилоотӣ-коммуникатсионӣ, балки соҳаи киберҷинояткорӣ низ босуръат рушд мекунанд. Таҳдидҳо ба захираҳои иттилоотӣ пайваста афзоиш ва инкишоф меёбанд. Аз ин рӯ самти асосии фаъолият дар муқовимат бо киберҷиноятҳо, ба андешидани тадбирҳои ташкилию техникии зерин асос меёбад:

1. Таъмини сатҳи зарурии амнияти системаҳо ва захираҳои иттилоотии давлатӣ, якпорчагӣ ва махфияти онҳо ба татбиқи талаботи ягона оид ба ҳифзи иттилоот аз дастрасии беиҷозат ё тағйир додани маълумот, таъсири ҳамлаҳои компютерӣ ва вирусҳо, инчунин истифодаи воситаҳои сертификатсияшудаи ватании пешгирӣ ва ошкор кардани ҳамлаҳои компютерӣ ва иттилооти муҳофизатӣ, ки аз ҷониби ташкилотҳое, ки бо тартиби муқарраршуда иҷозатномаи зарурӣ гирифтаанд;

2. Истифодаи воситаҳои криптографии ҳифзи иттилоот барои системаҳои иттилоотӣ ва захираҳои дорои маълумоти дорои сирри давлатӣ ҳатмӣ мебошад;

3. Назорат аз болои истифода ва ҳифзи системаҳо ва захираҳои давлатии иттилооти аз амалҳои ғайриқонунӣ бояд дар асоси ташкили системаи мониторингӣ ва баҳисобгирии амалиёт ҳангоми кор бо системаҳо ва захираҳои давлатии иттилооти таъмин карда шавад;

4. Таъмини муносибати маҷмуӣ ба ҳалли масъалаҳои амнияти иттилоотӣ аз ҳамлаҳои киберӣ бо дарназардошти зарурати тафриқаи сатҳи он дар мақомоти гуногуни давлатӣ;

5. Таҳияи модели таҳдидҳои амнияти иттилоотӣ аз ҳамлаҳои киберӣ;

6. Муайян намудани талаботҳои техникӣ ва меъёрҳои муайянкунии объектҳои муҳими инфрасохтори технологияҳои иттилоотӣ, ташкили феҳристи объектҳои муҳим, таҳияи чораҳои ҳифзи онҳо ва воситаҳои назорати риояи талаботи дахлдор;

7. Таъмини мониторинги самараноки ҳолати амнияти иттилоотӣ;

8. Такмили заминаи меъёрию ҳуқуқӣ ва методӣ дар соҳаи ҳифзи системаҳо ва захираҳои иттилоотии давлатӣ;

9. Ташкили тартиби ягонаи мувофиқа кардани шартҳои техникии таъмини амнияти иттилоотии системаҳо ва захираҳои иттилоотии давлатӣ;

10. Сертификатсияи системаҳо ва захираҳои давлатии иттилоотӣ дар фаъолияти мақомоти давлатӣ аз ҷониби мақомоти ваколатдори давлатӣ истифодашаванда ва назорати мутобиқати онҳо ба талаботи амнияти иттилоотӣ;

11. Ташкили сегменти алоқаи телекоммуникатсионӣ барои мақсадҳои махсус, таъмини имкони мубодилаи электронии иттилооти дорои сирри давлатӣ аз ҷониби мақомоти махсуси давлатӣ;

12. Ташаккули воситаҳои амнияти иттилоотӣ, системаҳои таъмини амнияти муомилоти ҳуҷҷатҳои электронӣ, системаи мониторинги амали хизматчиёни давлатӣ ҳангоми кор бо иттилоот, таҳия ва такмил додани воситаҳои коркарди иттилоот барои истифодаи умумӣ, системаҳои марказҳои сертификатсия дар соҳаи имзои электронии рақамӣ, ва инчунин системаи сертификатсия ва аудити онҳо.

Рисоланавис зикр менамояд, ки аз чораҳои умумии пешгирикунанда, ки ба пешгирии киберҷиноятҳо нигаронида шудаанд, инҳоро ҳамчун чораҳои афзалиятнок метавон номбар кард:

– истифодаи васеи имконияти ҳифзи шахсони воқеӣ ва ҳуқуқӣ;

– бо қонун манъ кардани шабакаҳои (ё компютерҳои ягонаи) объектҳои дорои аҳаммияти давлатӣ (стансияҳои барқии атомӣ, корхонаҳои мудофиа) бо Интернет. Рушди шабакаҳои идоравӣ ҷудо аз шабакаҳои умумии шаҳрвандӣ;

– муқаррар намудани манъи қонунгузорӣ оид ба истифодаи нармафзори тиҷоратӣ, ки бе рамзи ибтидоӣ дар соҳаи коркарди маълумоти махфӣ дода мешаванд;

– дар сатҳи қонунгузорӣ мустаҳкам намудани бартариҳои истеҳсолкунандагони нармафзор ҳангоми харидории барномаҳо аз ҷониби ташкилотҳои давлатӣ.

Ҳангоми ҳалли масъалаҳои пешгирии киберҷиноятқорӣ корҳои пешгирикунанда ба фароҳам овардани шарити мусоид равона карда мешаванд. Самаранокии ин равишро ҳам коршиносони ватанӣ ва ҳам хориҷӣ таъйид кардаанд, ки дуруст мешуморанд, ки пешгирии киберҷиноятҳо аз ошкор ва тафтиши он ҳамеша осон ва содатар аст.

ХУЛОСА

Дар асоси ҷамъбасти таҳлилу таҳқиқи илмӣ оид ба масъалаҳои ҳуқуқӣ-ҷиноятӣ ва криминологии муқовимат бо киберҷиноятҳо: проблемаҳои назариявӣ ва амалӣ дар тадқиқоти диссертатсионӣ мо ба хулосаи ниҳоӣ омада, пешниҳод менамоем:

1. Таҳаввулоти вирусҳои компютерӣ ҳамчун омили асосии ташаккули киберҷиноятҳо аз чунин марҳилаҳоро дар бар мегирад:солҳои 1970-1980; 1980-1992; 1992-2000; 2000 – то инҷониб [13-М].

2. Тараққиёти технологияҳои иттилоотӣ ва ворид шудани онҳо ба тамоми соҳаҳои ҳаёти инсон боиси пайдоиши шаклҳои нави киберҷиноятҳо

мегардад. Ин ҳолат зарурати андешидани чораҳои самарабахши муқовимат бо онҳо, ислоҳи қонунгузории ҷиноятии амалкунанда ва қабули меъёрҳои навро ба миён меорад [31-М].

3. Аз натиҷаи таҳлилҳои ҷойдошта мафҳуми киберҷиноятҳо пешбини гардидааст [12-М].

4. Киберҷиноятҳо тасниф карда мешаванд: а) вобаста ба объекти таҷовузи ҷиноятӣ; б) аз рӯйи хусусияти зарараре, ки ба иттилооти компютерӣ мерасонад; в) вобаста ба усулҳои содир намудани ҷиноят [10-М]; [2-М].

5. Конвенсияи Иттиҳодияи Аврупо оид ба киберҷиноятҳо ҳамчун, ягона Конвенсия, ки ҳамкории байналмилалӣ дар муқовимат бо киберҷиноятҳо эътироф гардидааст [15-М].

6. Марҳиллаҳои ҳамкорҳои байналмилалии Ҷумҳурии Тоҷикистон дар таъмини амнияти иттилоотӣ аз ҳамлаҳои киберӣ: солҳои 1992-2000; аз соли 2001 то ин ҷониб [16-М]; [27-М].

7. Аз таҳлили қонунгузории давалатҳои хориҷӣ муайян шудааст, ки сохтори таркибӣ ва мавқеи ҷойгиршавии киберҷиноятҳо дар низоми қонунгузории ҷиноятии давлатҳои хориҷӣ дар шаклҳои гуногун дида мешавад [6-М]; [20-М].

8. Объекти ҷиноятҳо муқобили шабакаҳои интернетӣ ва таҷҳизотҳои ёрирасони онҳо муносибатҳои ҷамъиятӣ дар самти ҷиноятҳо муқобили амнияти иттилоотӣ, кирдори шахс, манфиатҳои гуногуни шахсӣ ва иҷтимоӣ, инчунин ҳуқуқ ва манфиатҳои қонунан ҳифзшавандаи шаҳрвандон мебошад [25-М]; [2-М].

9. Объекти бевоситаи ҷиноятҳо муқобили шабакаҳои интернетӣ ва таҷҳизотҳои ёрирасони онҳоро муносибатҳои ҷамъиятие ташкил медиҳанд, ки дар натиҷаи содиршавиашон ба низоми ҳуқуқии дастрасӣ, истифода ва паҳнкунии иттилооти компютерӣ, ҳуқуқи соҳибии системаи компютерӣ, ба дахлнопазирии иттилооти компютерӣ (таъминоти барномавӣ), истифодаи бехатари мошинҳои ҳисоббарори электронӣ ва иттилооти компютерӣ ва кори муътадили компютерҳо, шабакаҳои интернетӣ, инчунин ба бехатарии истифодаи унсурҳои зеҳнӣ ва моддии мошинҳои ҳисоббарор заррар мерасад [2-М].

10 Тарафи объективии ҷиноятҳое, ки муқобили шабакаҳои интернетӣ ва таҷҳизотҳои ёрирасони онҳо муносибатҳои зоҳирии инсон ташкил медиҳанд, ки дар умум онҳоро ба ду гурӯҳ ҷудо кардан мумкин аст: Ҳамлаҳое, ки барои қатъи шабакаҳои алоқа ва роутерҳо нигаронида шудаанд; Ҳамлаҳое, ки ба пуррасозии системаи операторсионӣ ё захираҳои барнома нигаронида шудаанд [25-М]; [2-М].

11. Номгуи объекти ҷиноятҳое, ки тавассути воситаҳои гуногуни техникӣ содиршавандаро инҳо ташкил медиҳад: ҳуқуку озодиҳои конститутсионии инсон ва шаҳрванд (шаъну шараф, эътибор ва обрӯи шахс, дахолатнопазирии ҳаёти шахсӣ, сирри шахсӣ ва оилавӣ; маҳрамияти мукотиба, суҳбатҳои телефонӣ, мактубҳои почтавӣ, телеграфӣ, ҳуқуқҳои муаллифӣ ва ҳуқуқҳои вобаста ба он); иттилооти компютерӣ ва технологияҳои иттилоотӣ;

амният дар соҳаи иқтисодиёт, ҳокимияти давлатӣ, ҳаёт ва саломатӣ ва ахлоқи ҷамъиятӣ.

12. Тарафи объективии ҷиноятҳоеро, ки тавассути воситаҳои гуногуни техникӣ содир мешаванд ин муносибатҳои зоҳирии шахсро оид ба ғайриқонунӣ ҷамъ ва паҳн кардани маълумот дар бораи шахси дигар, ба тавр и оммавӣ ва ё дар воситаҳои ахбори омма намоиш додани ин маълумот, инчунин ирсоли мактубҳо бо роҳи фиреб тавассути шабакаи интернетӣ ташкил медиҳанд, ки ҳангоми содиршавиашон ба ҳуқуқ ва манфиатҳои қонунии шаҳрвандон заррар расонида мешавад [29-М].

13. Тарафи субъективии ҷиноятҳое, ки тавассути воситаҳои гуногуни техникӣ содир мешаванд танҳо бо гуноҳ дар шакли қасди бевосита ҷой дошта метавонанд [21-М].

14. Номгуи субъектони ҷиноятҳое, ки бо истифода аз воситаҳои гуногуни техникӣ содир мешаванд, дар умум субъекти умумӣ, яъне шахси воқеии мукаллафи ба сину соли муқарраршуда расида шуда метавонанд. Вале онҳоро шартан ба ду гурӯҳ ҷудо кардан мумкин аст. 1. Шахсоне, ки дорои донишҳои махсус дар самти ТИК ва барномасозӣ мебошанд (провайдерон, хакерон, операторон, барномасозон ва ғ.); 2. Шаҳрвандони оддӣ. Ин намуди ҷиноятҳоро метавонанд шахсоне содир кунанд, ки бо фаъолияти умумии шабакаи интернетӣ шинос буда онро ба қадри кофӣ ҳамарӯза истифода менамоянд. Дар маҷмуъ, дар эътирофи сукбъекти ин ҷиноятҳо муҳим корманди ин ё он ташкилот ё муассиса будан нест, балки истифодабарандаи шабакаҳои интернетӣ бошад [29-М].

15. Дар натиҷаи баррасии маълумотҳои оморӣ ва таҳқиқи парвандаҳои ҷиноятӣ вобаста ба масъалаҳои криминологии киберҷиноятҳо ба чунин хулосаи ниҳоӣ омадан зарур аст:

– яке аз тамоюлҳои асосии рушди киберҷинояткорӣ саривақт ошкор накардани он мебошад. Раванди роҳандозии ғайриқонунии шабакаҳои иттилоотию коммуникатсионӣ, мессенҷерҳои фаврӣ ва интернет ба ин раванд мусоидат мекунанд. Истифодаи технологияи навин дар муомилоти молиявӣ ва қарзӣ, тиҷорати онлайнӣ, рамзгузории маълумот ва ғайра ба давлат ва ҷомеа имкон намедиҳад, ки шумораи зиёди киберҷиноятҳоро саривақт пешгирӣ кунанд, зеро онҳо бо сабабҳои технологӣ сарфи назар карда мешаванд.

– надонистани қурбониёни киберҷиноятҳо аз воситаҳо ва усулҳои асосии ҳифзи иттилооти худ, ба ҳамлагар имкон медиҳад, ки ба осонӣ амалҳои ғайриқонунӣ содир кунад. Вобаста ба ин, инъикоси нақшаҳои маъмултарини киберҷиноятҳо ва роҳҳои пешгирӣ аз онҳо дар ВАО, инчунин дар байни аҳолӣ ташаккул додани малакаҳои коркарди иттилооти компютерӣ ва омӯзиши кор бо дастгоҳҳои гуногуни техники аз ҷумла интернет аҳаммияти муайян дорад.

– дараҷаи баланди киберҷиноятҳо бештар ба душвории ошкор кардани кирдори киберҷинояткор ва худдории ҷабрдида барои хабар додан ба мақомоти ҳифзи ҳуқуқ алоқамандӣ дорад [28-М].

– киберҷиноятқорон дар самти истифодаи интернет, воситаҳои гуногуни техникӣ ва таҳияи барномаҳои зараровар дониши васеъ доранд. Аз ин рӯ, мубориза бо киберҷиноятқорӣ бояд бо ҷалби мутахассисоне сурат гирад, ки ин хусусиятҳоро мавриди омӯзиш қарор дода бошад.

– содиршавии киберҷиноятҳо бо истифода аз ТИК дар айни замон рӯ ба афзоиш дорад. Аз ин лиҳоз зарур аст, ки вобаста ба таҳия ва қабул гардидани барномаҳои таълимӣ ва стандартҳои давлатӣ дар ин самт, зиёд тайёр кардани шумораи мутахассисон дар самти амнияти киберӣ, баланд бардоштани малакаи касбӣ ва маҳорати кормандоне, ки дар ин самт фаъолият мекунанд, ҷалби олимони соҳа, мутахассисони собиқадори техникӣ, инчунин ташкили институти такмили ихтисоси соҳаи таъмини амнияти иттилооти аз ҳамлаҳои киберӣ чораи махсус андешида шавад.

– ҳаҷми воқеӣ ва хусусияти ҳамлаҳои киберӣ пурра дар Сармаркази иттилоотӣ-таҳлилии Вазорати корҳои дохилии Ҷумҳурии Тоҷикистон инъикос нагардидаанд Бинобар ин фаъолияти ин Сармарказ дар ин самт ҷоннок карда шавад;

– аксари ҷабрдидагони киберҷиноятҳо шахсони ҳуқуқӣ мебошанд. Вобаста ба ин, корхонаю ташкилотҳоро зарур аст, ки ба таъмини амнияти компютерӣ аз ҳамлаҳои киберӣ таваҷҷуҳи ҷиддӣ дода, дар нақшаи корӣ вазифаи мутахассисони соҳавиро муайян намуда, баҳри пешгирии ҳар гуна ҳамлаҳои киберӣ бо истифода аз технологияи навини муосир чораҳо андешанд.

– таҳдиди бузургтарин ба амнияти иттилооти компютерии ҳифзшуда аз ҷониби корбарони дохилии системаи иттилоотӣ мебошад. Вобаста ба ин, такмил додани дараҷаи касбии мутахассисон ва мониторинги эътимоднокии онҳо аз ҷониби хадамоти амнияти мақомоти дахлдор аҳаммияти хоса дорад.

16. Омилҳои асосии ҳуқуқӣ-ҷиноятии ҳифзи ТИК аз амалҳои ҷиноятқорона инҳоянд: дар қонунгузори инъикоси усулҳои аз ҷиҳати технологии нави содир намудани кирдорҳои ғайриқонунӣ бо истифода аз технологияҳои киберӣ ва оқибатҳои эҳтимолии онҳо, махсусан амалҳои ғайриқонуни нисбат ба системаҳои киберфизикӣ, ба монанди бозdоштани назорат ва иғвоангезии интеллектуалӣ, осеб дидани таҷҳизоти тиббӣ бо истифода аз ҳамлаи компютерӣ, вайрон кардани системаҳои хидмарасониҳои ҳаётан муҳим; аз ҷумла онҳое, ки тавассути инфрасохтори таҳсимшудаи фаромарзӣ сурат мегиранд; аз ҷониби мақомоти дахлдор баррасии масъалаи ворид намудани иловаҳо ба қонунгузории ҷиноятӣ вобаста ба кирдорҳои ғайриқонунӣ, ки бо истифода аз воситаҳои технологӣ содир шудаанд; дар муқовимат бо киберҷиноятқорӣ ба мафҳуми «далеловариҳои рақамӣ» (digitalevidence), инчунин ҳамоҳангсозии ин ё он равия ва баррасии онҳо дар ҷараёни тафтиши парвандаҳои ҷиноятӣ ва баррасии онҳо аз ҷониби судҳо ҳамчун далели шайъӣ диққати махсус дода шавад; таваҷҷуҳи асосӣ бояд ба раванди ҷорӣ намудани стратегия ва принсипҳои муқовимати фаъолона бо киберҷиноятқорӣ равона карда шавад, то шароити мусоид ба мубоизаи чу-

нин кирдорҳои барои ҷамъият хавфнок аз ҷониби мақомоти ҳифзи ҳуқуқ таъмин карда шавад; ҳамкории дурусти байниидоравии низоми мақомоти ҳифзи ҳуқуқ дар гузаронидани санҷишҳои молиявӣ, пешгирии ҳама шаклҳои қаллобӣ ва тасарруфи маблағҳо, инчунин ба роҳ мондани ҳамкории мутақобилан судманди байналмилалӣ аз ҷониби ин мақомотҳо; таҳияи барномаҳо ё стратегияҳо ҳамчун маҷмуи чораҳои пешгирикунанда, омодасозии системаи дахлдор ба мақомоти ҳифзи ҳуқуқ дар мубориза бо ин ҷиноятҳо, инчунин баррасии масъалаи ҳифзи кӯдакон аз ҳар гуна таҷовузҳо, ки тавассути шабакаҳои интернетӣ содир мешаванд [22-М]; [28-М].

17. Азбаски технологияҳои иттилоотӣ айни замон макони ҷойгиршавии муайян надоранд ва дар ин маврид корбарони ғайриқонунӣ аз маълумоти дигарон аз дилхоҳ ҷой истифода менамоянд, роҳандозии чораҳои зерин ба манфиати кор мебошад:

Дар сатҳи миллӣ:

– иштироки давлат дар таҳияи стратегияи байналмилалии муқовимат бо таҳдидҳои киберӣ ва ташкили механизмҳои ягонаи ҳуқуқии байналмилалии танзими фазои маҷозӣ;

– лоиҳаи Консепсияи миллии ё Стратегияи давлатии таъмини амнияти киберӣ бояд таҳия карда шавад, ки ба принсипҳо ва меъёрҳои қонунгузорӣ асос ёфта, татбиқи онро дар сатҳи зарурӣ ва соҳаҳои гуногуни давлатӣ фарогир бошад;

– таҳия ва татбиқи низоми бисёрсатҳи институтсионалии амнияти киберӣ, ки ин омилҳоро фаро мегирад: 1) сатҳи илмӣ ва таҳлилӣ, ки мувофиқи он хатарҳои киберӣ вобаста бо эҳтимолияти рух додани таҳдидҳои киберӣ ва миқёси оқибатҳои манфӣ омухта мешавад; 2) сатҳи амалӣ, ки дар ду самт ҳамоҳанг хоҳад шуд – дохилӣ (байни сохторҳои мақомоти давлатӣ, ки барои муайян ва муқовимат бо таҳдидҳои киберӣ масъул мебошанд) ва берунӣ, ки дар доираи ҳамоҳангсозии сохторҳои давлатӣ ва институтҳои минтақавӣ ва байналмилалӣ амалӣ карда мешавад;

– баланд бардоштани иқтидори соҳаи иттилоот оид ба мубориза бар зидди ҳамлаҳои киберӣ, ки тадбирҳои сиёсии дохилиро вобаста ба технологияи амнияти киберӣ пурзӯр менамояд;

– ҳимоя, яъне амалӣ ва татбиқи ҳамкориҳои минтақавӣ ва байналмилалӣ дар соҳаи амнияти киберӣ, пайгирии фаъолияти гурӯҳҳои ҷиноятӣ, террористӣ, ки дар фазои маҷозӣ амал мекунанд;

– барои рушди ҳамкориҳои байналмилалӣ сохторҳое, ки ба муайян намудани таҳдидҳои киберӣ, сари вақт ошкор, пешгирӣ, ҳифз ва кам кардани оқибатҳо нигаронида шудаанд, бояд фаъолона иштирок намоянд.

Дар сатҳи байналмилалӣ:

– таҳия ва татбиқи созишномаи байналмилалӣ дар соҳаи пешгирӣ ва тафтиши ҳамлаҳои киберӣ миёни ҶТ ва давлатҳои хориҷӣ;

– таъсиси як ниҳоди байналмилалӣ бо намояндагиҳои минтақавӣ. Ин ниҳод бояд доираи Созмони Милали Муттаҳид дар фазои маҷозӣ буда, як-

чанд сохторро фарогир бошад, масалан: барномаҳо ё консепсияҳоро дар ин самт қабул намояд, нақша-чорабиниҳоро тарҳрезӣ намояд, иҷрои вазифаҳоеро, ки бояд дар сатҳи давлатӣ ягона бошанд амалӣ намояд ва ғ. [9-М].

Тавсияҳо оид ба истифодаи амалии натиҷаҳои таҳқиқот

1. Зарур аст, ки барномаҳои таълимӣ ва стандартҳои давлатӣ дар самти таъмини амнияти иттилооти аз ҳамлаҳои киберӣ, қабул гардидад [17-М]; [18-М].

2. Дар заминаи муассисаҳои таҳсилоти олии мамлакат, ихтисоси «амнияти киберӣ» ҷорӣ карда шавад [30-М].

3. Фаъолияти кории Шурои Технологияи иттилоотию коммуникатсионии назди Президенти Ҷумҳурии Тоҷикистон, таҷдид карда шуда, дигар шуроҳои дар ин замина ташкил гардида, ҷиҳати ба он интиқол додани вазифаҳои ҳамоҳангсозӣ ва роҳбарии байнисоҳавии субъектони муқовимат бо киберҷиноятҳо (аз ҷумла, Прокуратураи генераии ҶТ, КДАМ ҶТ, ВКД ҶТ ва Вазорати адлияи ҶТ) муқарар карда шавад.

4. Бо дарназардошти вазъи мураккабу ташвишовари минтақа ва ҷаҳон, инчунин ҷамъоварӣ ва коркарди маълумот оид ба киберҷиноятҳо, гузаронидани арзёбии экспертии таҳдидҳои киберӣ, таҳия ва татбиқи усулҳои пешрафтаи пешгирӣ ва тафтиши киберҷиноятҳо, дар доираи СПАД «Маркази муқовимат бо киберҷиноятҳо», ҳамчун мақомоти махсусгардонидашуда таъсис дода шавад [24-М].

5. Маркази ягонаи коммутатсионии алоқаи барқии Хадамоти алоқаи назди Ҳукумати ҶТ, Прокуратураи генералии ҶТ ва Вазорати корҳои дохилии ҶТ–ро зарур аст, ки бо мақсади таъмини амнияти иттилооти аз ҳамлаҳои киберӣ дар мамлакат, дастрасиро ба сомонаҳо ва захираҳои дигари иттилоотӣ (аз ҷумла сомона ва барномаҳои интернетӣ, ки ба паҳн намудани ҳама гуна иттилоот бар зидди асосҳои сохтори конститутсионӣ, амнияти шахсӣ, ҷамъиятӣ, давлатӣ, паст задани шаъну эътибори миллӣ), маҳдуд намоянд.

6. Барои хусусияти меъёриро касб намудани мафҳуми киберҷиноятҳо, амнияти киберӣ, фазои маҷозӣ, объекти иттилоот, таҳдиди киберӣ, объекти амнияти киберӣ, субъекти таъмини амнияти киберӣ, ҳамлаҳои киберӣ, сиёсати ягонаи давлатӣ дар соҳаи амнияти киберӣ, мақомоти ваколатдори давлатӣ дар соҳаи амнияти киберӣ, ҳуқуқ ва уҳдадориҳои мақомоти ваколатдори давлатӣ дар соҳаи амнияти киберӣ, системаи таъмини амнияти киберӣ, дастгирии илмӣ-техникӣ ва инноватсионӣ дар соҳаи амнияти киберӣ ва ҳамкории байналмилалӣ дар соҳаи амнияти киберӣ зарур медонем, ки Қонуни Ҷумҳурии Тоҷикистон «Дар бораи амнияти киберӣ» қабул карда шавад [26-М].

7. Бо мақсади такмили қонунгузории ҷиноятӣ ва мустаҳкам гардонидани омилҳои муқовимат бо киберҷиноятҳо ба КҶ ҶТ тағйирот ворид кард шавад. Махсусан дар боби 28 КҶ ҶТ чунин пешниҳодҳоро вобаста ба тағйиру иловаҳо дар қонунгузории ҷиноятӣ зарур мешуморем:

а) моддаи 298 (1). Ба даст овардани маълумоти электронии шахсӣ бо роҳи фиреб ё усулҳои дигари дастрасии ғайриқонунӣ ба маълумот барои истифода ба манфиати шахсӣ;

б) моддаи 300. Кодекси ҷиноятии ҶТ, қисми 2 дар таҳрири нав илова карда шавад;

в) дар боби 28-и КҶ ҶТ моддаи 300 (1) Ҳамлаи компютерии DoS ва Моддаи 301 (2). Ғайриқонунӣ дар шакли оммавӣ паҳн кардани паёмҳои электронӣ моддаҳои нав, ворид карда шавад;

г) ба мақсад мувофиқ аст, ки қисми 3-юми моддаи 301 КҶ ҶТ бандҳои алоҳида илова карда шавад;

д) моддаи 301 (3). Таҳия, интишор ва паҳн кардани иттилоот, бо истифодаи шабакаи интернет ва ҳама гуна воситаҳои шабакаҳои иттилоотию телекоммуникатсионӣ дар КҶ ҶТ ворид карда шавад;

е) зарурияти ворид намудани тағйирот ба қисми 2 моддаи 302 КҶ Ҷ ба миён омадааст;

ё) пешниҳод карда мешавад, ки моддаи 303-и Кодекси ҷиноятии Ҷумҳурии Тоҷикистон дар таҳрири нав ифода карда шавад: Моддаи303. Ғайриқонунӣ таҳия, истифода ё паҳн кардани барномаҳои зараровари компютерӣ.

8. Аз баррасӣ ва таҳлили объекти ҷиноятҳо муқобили шабакаҳои интнренети ва таҷҳизотҳои ёрирасони онҳо мувофиқи мақсад мешуморем, фасли нав дар КҶ ҶТ бо номи «Ҷиноятҳо муқобили амнияти киберӣ» ворид карда шавад [25-М].

ФЕҲРИСТИ ИНТИШОРОТИ ИЛМИИ ДОВТАЛАБИ ДАРАҶАИ ИЛМӢ

I. Монографияҳо:

[1-М]. Раджабов, К.Д. Уголовно-правовые и криминологические проблемы борьбы с вымогательством [Текст]: монография / К.Д. Раджабов. –Душанбе: «Лахути», 2020. – 156 с. (9,75 п.л.); ISBN 978-99975-358-7-0.

[2-М]. Давлатзода, К.Д. Таҳдидҳои фазои маҷозӣ: амалия ва назарияи киберҷиноятҳо [Матн]: монография / К.Д. Давлатзода. – Душанбе: «Матбааи ДМТ», 2023. – 248 с. (15,5 ч.ч.); ISBN 978-99985-41-01-6.

II. Мақолаҳое, ки дар маҷаллаҳои тақризшаванда ва тавсиякардаи Комиссияи олии аттестатсионии назди Президенти Ҷумҳурии Тоҷикистон ба табъ расидаанд:

[3-М]. Раджабов, К.Д. Развитие понятия вымогательства в уголовном праве [Текст] / К.Д. Раджабов // Вестник Таджикского национального университета. – 2017. – №2/7. – С. 237-241; ISSN 2413-5151.

[4-М]. Раджабов, К.Д. Объективная сторона вымогательства [Текст] / К.Д. Раджабов // Вестник Таджикского национального университета. – 2018. – №2. – С. 210-214; ISSN 2413-5151.

[5-М]. Давлатзода, К.Д. Масоили таърихӣ ва назариявии ташаккули ҷиноятҳои компютерӣ [Матн] / К.Д. Давлатзода // Қонунгузорӣ. – 2021. – №4 (44). – С. 92-95; ISSN 2410-2903.

[6-М]. Давлатзода, К.Д., Назаров, А.Қ. Таҳлили муқоисавии ҳуқуқи ҷиноятӣ дар самти мубориза бар зидди ҷиноятҳои компютерӣ дар кишварҳои аъзои ИДМ ва дигар давлатҳои хориҷӣ [Матн] / К.Д. Давлатзода, А.Қ. Назаров // Паёми Донишгоҳи миллии Тоҷикистон. Бахши илмҳои иҷтимоӣ-иқтисодӣ ва ҷамъиятӣ. – 2022. – №3. – С. 229-236; ISSN 2413-5151.

[7-М]. Давлатзода, К.Д., Назаров, А.Қ. Истифодаи технологияи рақамӣ дар фаъолияти оперативӣ-ҷустуҷӯӣ [Матн] / К.Д. Давлатзода, А.Қ. Назаров // Паёми Донишгоҳи миллии Тоҷикистон. Бахши илмҳои иҷтимоӣ-иқтисодӣ ва ҷамъиятӣ. – 2022. – №4. – С. 207-212; ISSN 2413-5151.

[8-М]. Давлатзода, К.Д. Праблемаҳои ҳуқуқии-ҷиноятии мафҳуми ғайриқонунӣ ба даст овардани иттилооти компютерӣ [Матн] / К.Д. Давлатзода // Давлатшиносӣ ва ҳуқуқи инсон. – 2022. – №1 (25). – С. 179-187; ISSN 2414 9217.

[9-М]. Давлатзода, К.Д. Ҷаҳонишавии проблемаҳои киберҷиноятҳо [Матн] / К.Д. Давлатзода // Паёми Донишгоҳи миллии Тоҷикистон. Бахши илмҳои иҷтимоӣ-иқтисодӣ ва ҷамъиятӣ. – 2022. – №9. – С. 231-237; ISSN 2413-5151.

[10-М]. Давлатзода, К.Д. Таснифоти киберҷиноятҳо [Матн] / К.Д. Давлатзода // Паёми Донишгоҳи миллии Тоҷикистон. Бахши илмҳои иҷтимоӣ-иқтисодӣ ва ҷамъиятӣ. – 2022. – №8. – С. 279-284; ISSN 2413-5151.

[11-М]. Давлатзода, К.Д. Танзими ҳуқуқии муносибатҳо дар соҳаи иттилооти компютерӣ [Матн] / К.Д. Давлатзода // Қонунгузорӣ. – 2022. – №2 (46). – С. 117-122; ISSN 2410-2903.

[12-М]. Давлатзода, К.Д. Таҳқиқоти ҳуқуқии ҷиноятии мафҳуми киберҷиноятҳо [Матн] / К.Д. Давлатзода // Давлатшиносӣ ва ҳуқуқи инсон. – 2022. – №3 (27). – С. 428-434; ISSN 2414 9217.

[13-М]. Давлатзода, К.Д. Таҳаввулоти вирусҳои компютерӣ ҳамчун омили асосии пайдоиш ва содишавии киберҷиноятҳо [Матн] / К.Д. Давлатзода // Паёми Донишгоҳи давлатии Данғара. – 2022. – №4 (22). – С. 138-144; ISSN 2410-4221.

[14-М]. Давлатзода, К.Д. Кибертерроризм ҳамчун намуди нави амали террористӣ [Матн] / К.Д. Давлатзода // Паёми Донишгоҳи миллии Тоҷикистон. Бахши илмҳои иҷтимоӣ-иқтисодӣ ва ҷамъиятӣ. – 2023. – №1. – С. 207-213; ISSN 2413-5151.

[15-М]. Давлатзода, К.Д. Аҳаммияти санадҳои байналмилалӣ дар муқовимат бо киберҷиноятҳо [Матн] / К.Д. Давлатзода // Паёми Донишгоҳи миллии Тоҷикистон. Бахши илмҳои иҷтимоӣ-иқтисодӣ ва ҷамъиятӣ. – 2023. – №2. – С. 221-229; ISSN 2413-5151.

[16-М]. Давлатзода, К.Д. Ҳамкориҳои минтақавии Ҷумҳурии Тоҷикистон дар самти мубориза бо киберҷиноятҳо: дар мисоли Созмони

ҳамкории Шанхай ва Созмони паймони амнияти дастаҷамъӣ [Матн] / К.Д. Давлатзода // Паёми Донишгоҳи миллии Тоҷикистон. Бахши илмҳои иҷтимоӣ-иқтисодӣ ва ҷамъиятӣ. – 2023. – №6. – С. 232-237; ISSN 2413-5151.

[17-М]. Давлатзода, К.Д. Тавсифи ҳуқуқии ҷиноятии савдои одамон дар фазои киберӣ [Матн] / К.Д. Давлатзода // Паёми Донишгоҳи миллии Тоҷикистон. Бахши илмҳои иҷтимоӣ-иқтисодӣ ва ҷамъиятӣ. – 2023. – №8. – С. 228-234; ISSN 2413-5151.

[18-М]. Давлатзода, К.Д. Порнографияи кӯдакон дар Интернет: мафҳум, оқибат ва масъалаҳои ҳуқуқии ҷиноятии мубориза бар зидди он [Матн] / К.Д. Давлатзода // Паёми Донишгоҳи миллии Тоҷикистон. Бахши илмҳои иҷтимоӣ-иқтисодӣ ва ҷамъиятӣ. – 2023. – №9. – С. 244-249; ISSN 2413-5151.

[19-М]. Давлатзода, К.Д. Тамаъҷӯӣ дар фазои маҷозӣ: мафҳум ва хусусиятҳои он [Матн] / К.Д. Давлатзода // Қонунгузорӣ. – 2023. – №3 (51). – С. 144-150; ISSN 2410-2903.

[20-М]. Давлатзода, К.Д. Ҷавобгарии ҷиноятӣ барои киберҷиноятҳо тибқи қонунгузории Ҷумҳурии Мардумии Чин: таҳлили муқоисавии ҳуқуқӣ [Матн] / К.Д. Давлатзода // Осори Академияи ВКД Ҷумҳурии Тоҷикистон. – 2023. – №3 (59). – С. 31-36; ISSN 2412-141X.

[21-М]. Давлатзода, К.Д. Нишонаҳои тарафи субъективии ҷиноятҳо ба муқобили шабакаҳои интернетӣ ва таҳҳизотҳои ёрирасони онҳо ҳамчун намуди нави киберҷиноятҳо (барномаҳои зараровар ва ҳамлаҳои DoS) [Матн] / К.Д. Давлатзода // Паёми Донишгоҳи миллии Тоҷикистон. Бахши илмҳои иҷтимоӣ-иқтисодӣ ва ҷамъиятӣ. – 2023. – №10. – С. 233-240; ISSN 2413-5151.

[22-М]. Давлатзода, К.Д. Тавсифи криминалогии шахсияти киберҷинояткор [Матн] / К.Д. Давлатзода // Қонунгузорӣ. – 2023. – №4 (51). – С. 211-217; ISSN 2410-2903.

III. Мақолаҳои илмие, ки дар маҷмуаҳо ва дигар нашрияҳои илмӣ-амалӣ чоп шудаанд:

[23-М]. Давлатзода, К.Д., Назаров, А.Қ. Нақши тафаккури сунъӣ дар раванди амалишавии фаъолияти оперативӣ-чустуҷӯӣ [Матн] / К.Д. Давлатзода, А.Қ. Назаров // Криминалистикаи муосир: маводи конференсияи ҷумҳуриявии илмӣ-амалӣ // Зери назари умумии н.и.ҳ., дотсент Ф.Р. Шарифзода. – Душанбе: Нашриёти ВКД Ҷумҳурии Тоҷикистон, 2022. – С. 111-117.

[24-М]. Давлатзода, К.Д., Назаров, А.Қ. Ташкилотҳои байналмилалӣ ҳамчун субъектони муқовимат бо киберҷиноятҳо [Матн] / К.Д. Давлатзода, А.Қ. Назаров // Маводи конференсияи байналмилалии илмӣ-амалӣ бахшида ба 25-солагии Кодекси ҷиноятии Ҷумҳурии Тоҷикистон: ҳолат ва дурнамо. – Душанбе: Нашриёти ВКД Ҷумҳурии Тоҷикистон, 2023. – С. 143-148.

[25-М]. Давлатзода, К.Д. Барномаҳои зараровар ҳамчун воситаи содиршавии киберҷиноятҳо: мафҳум ва намудҳои он [Матн] / К.Д. Давлатзода // Маҷмуи мақолаҳои конференсияи ҷумҳуриявии илмию-амалӣ дар мавзуи

«Мушкилотҳои қонунгузории замин дар даврони муосир». – Душанбе, 2023. – С. 235-238.

[26-М]. Давлатзода, К.Д. Таҳдидҳои кибернӣ: қаллобӣ дар фазои маҷозӣ [Матн] / К.Д. Давлатзода // Маҷмуи мақолаҳои конференсияи байналмилалӣ дар мавзуи «Тоҷикон дар оинаи таърих», бахшида ба 115 солагии академик Бобоҷон Ғафуров (Филиали Донишгоҳи давлатии Москва ба номи Михаил Ломоносов дар шаҳри Душанбе). – Душанбе, 2023. – С. 61-64.

[27-М]. Давлатзода, К.Д. Ташаббусҳои байналмилалии Ҷумҳурии Тоҷикистон дар таъмини амнияти иттилоотӣ аз ҳамлаҳои кибернӣ [Матн] / К.Д. Давлатзода // Маводи конференсияи байналмилалии илмию амалии «Илм ва таҳсилот: тамоюлҳои рушд дар ҷомеаи иттилоотӣ» бахшида ба «75-солагии ДМТ». – Душанбе, 2023. – С. 405-409.

[28-М]. Давлатзода, К.Д. Хакер: тавсифи криминологии он [Матн] / К.Д. Давлатзода // Масоили мубрами такмили Конститутсияи Ҷумҳурии Тоҷикистон дар шароити муосир: маводи конференсияи чумҳурявии илмию назариявӣ бахшида ба 75-солагии Донишгоҳи миллии Тоҷикистон. – Душанбе, 2023. – С. 227-233.

[29-М]. Давлатзода, К.Д. Интернет воситаи содиршавии кибертаъқиб [Матн] / К.Д. Давлатзода // Ҳифзи ҳуқуқи инсон ва масъалаи муқовимат ба коррупсия дар ҷаҳони муосир: консепсияҳо, воқеият ва дурнамо: маводи конференсияи байналмилалии илмӣ-амалӣ бахшида ба 75-умин солгарди қабули Эъломияи умумии ҳуқуқи инсон ва рӯзи байналмилалии мубориза бар зидди коррупсия (Академияи идоракунии давлатии назди Президенти ҶТ). – Душанбе, 2023. – С. 189-169.

[30-М]. Давлатзода, К.Д. Таҳлили таҷрибаи амалии мақомоти ваколатдори давлатӣ ва ҳамкории байналмилалии онҳо дар самти таъмини амнияти кибернӣ [Матн] / К.Д. Давлатзода // Масъалаҳои назариявии ташаккули фарҳанги ҳуқуқи инсон дар Тоҷикистон: маводи конференсияи байналмилалии илмию назариявӣ. – Душанбе, 2023. – С. 280-289.

IV. Воситаи таълимӣ:

[31-М]. Давлатзода, К.Д. Асосҳои тафтиши киберҷиноятҳо [Матн]: воситаи таълимӣ / К.Д. Давлатзода. – Душанбе: «Матбааи ДМТ», 2023. – 150 с. (9,3 ҷ.ч.); – ISBN 978-99985-41-11-5.

ТАДЖИКСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ

На правах рукописи

УДК:343 (575.3)

ДАВЛАТЗОДА КОМРОН ДАВЛАТ

УГОЛОВНО-ПРАВОВЫЕ И КРИМИНОЛОГИЧЕСКИЕ ВОПРОСЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ: ТЕОРЕТИЧЕСКИЕ И ПРАКТИЧЕСКИЕ ПРОБЛЕМЫ

АВТОРЕФЕРАТ
диссертации на соискание ученой степени доктора юридических наук
по специальности 12.00.08 – Уголовное право и криминология;
уголовно-исполнительное право

ДУШАНБЕ – 2024

Диссертация выполнена на кафедре криминалистики и судебно-экспертной деятельности юридического факультета Таджикского национального университета.

Научный консультант: **Назаров Аваз Кувватович** – доктор юридических наук, доцент, заведующий кафедрой криминалистики и судебно-экспертной деятельности юридического факультета Таджикского национального университета

Официальные оппоненты: **Абдухамитов Валижон Абдухамитович** – доктор юридических наук, профессор кафедры уголовного права Российско-Таджикского (Славянского) университета;

Салаев Нодирбек Сапарбаевич – доктор юридических наук, доцент, профессор кафедры уголовного права, криминологии и противодействия коррупции Ташкентского государственного юридического университета;

Азимзода Назир Бозор – доктор юридических наук, профессор, заведующий кафедры международного отношения и права Международный университет иностранных языков Таджикистана имени Сотим Улугзаде.

Ведущее учреждение: Образовательное учреждение высшего профессионального образования «Академия МВД Республики Таджикистан» (г. Душанбе).

Защита диссертации состоится «22» июня 2024 года в $10^{\underline{00}}$ часов на заседании диссертационного совета 6D.КОА-019 при Таджикском национальном университете (734025, г. Душанбе, ул. Буни Хисорак, зал диссертационного совета юридического факультета).

С диссертацией можно ознакомиться на сайте www.tnu.tj и в Центральной научной библиотеке Таджикского национального университета по адресу 734025, г. Душанбе, пр. Рудаки 17.

Автореферат разослан: «___» _____ 2024 года.

Ученый секретарь диссертационного совета,
доктор юридических наук, профессор **Гадоев Б.С.**

ВВЕДЕНИЕ

Актуальность темы исследования. Обеспечение информационной безопасности от кибератаки в условиях глобализации стало актуальным вопросом, а информация стала особо защищаемым объектом. В связи с этим, в целях совершенствования отношений в области безналичных расчетов в условиях бурного развития информационно-коммуникационных технологий в отечественных финансово-кредитных организациях используются современные цифровые финансовые технологии, такие как банковские платежные карты, электронные кошельки, мобильный банкинг, интернет-банкинг, платежи через POS-терминал и QR-код, применяют код, который в этом контексте в большей степени зависит от информационных ресурсов, информационных и телекоммуникационных сетей. Также налажена система предоставления государственных и коммунальных услуг в электронной форме, что обеспечивает благоприятные условия для повышения международного рейтинга страны и привлечения иностранных инвестиций.

Следует отметить, что информационные и коммуникационные технологии оказывая большое влияние на развитие различных отраслей экономики, становятся частью современных систем управления во всех секторах экономики, государственного управления, обороны, государственной безопасности и защиты прав человека.

Особую роль играет широкое внедрение информационно-коммуникационных технологий (далее ИКТ) во все сферы жизнедеятельности человека, правовое регулирование использования ИКТ и защита информационных ресурсов. В современном мире информатизация общества продолжается очень высокими темпами, а киберпреступления, кибератаки на информационные системы, незаконный доступ к информационным ресурсам, хранящимся в памяти компьютеров, представляют реальную угрозу безопасности личности, общества, государства и их законным интересам.

В последние годы мы стали свидетелями того, что с развитием информационных технологий и развитием сетей Интернет появляются новые средства связи между коммуникаторами. Интернет-общение принимая разные формы оказывает влияние на все сферы мирового сообщества. Интернет имеет глобальное влияние на современную повседневную жизнь и, в зависимости от цели его использования, может приводить к опасным к социальным последствиям. Необходимые материалы доступны виртуально и в любой момент. Можно найти соответствующие ответы на вопросы из разных областей с разным уровнем сложности. Также есть много других примеров, которые можно назвать в этом случае. К сожалению, при ненадлежащем использовании, развитие технологий может повлечь за собой нанесение ущерба членам общества и привести к появлению и совершенствованию различных киберзапугиваний и угроз, которые не всегда видимы и раскрываемы. Однако проблема предотвращения и противодействия этим нежелательным явлениям связана, в частности, с их невидимой природой.

В этом контексте относительно актуальности данного исследования Основатель мира и национального единства – Лидер нации, Президент Республики Таджикистан, уважаемый Эмомали Рахмон в своем ежегодном Послании Маджлиси Оли «Об основных направлениях внутренней и внешней политики Республики», которое состоялось 28 декабря 2023 года, подчеркнул, что сложная и тревожная ситуация в регионе и мире, в том числе обострение процесса перераспределения мира, вооружения, «холодной войны», современные угрозы и опасности – терроризм, экстремизм, киберпреступность и другие организованные транснациональные преступления побуждают нас принять дополнительные меры для обеспечения безопасности обороны нашей страны. В то же время, 28 декабря 2022 года на торжественном заседании, посвященном профессиональному празднику сотрудников органов национальной безопасности Республики Таджикистан, Лидер нации, уважаемый Эмомали Рахмон, справедливо отметил, что «Вызовы киберпреступности и кибертерроризма как новых угроз оказывают серьезное негативное влияние на международную безопасность. В этой связи органам безопасности необходимо быть бдительными как никогда, регулярно изучать и анализировать процессы и события в регионе и мире, принимать законные, необходимые и срочные меры по пресечению планов, направленных на подрыв безопасности государств и обществе мирной жизни людей…»[1].

До 2008 года на территории РТ на было зарегистрировано ни одного киберпреступления. В 2008 было зарегистрировано два преступления в вышеуказанной сфере. В целом с 2009 по 2023 гг. количество совершаемых преступлений в сфере кибербезопасности резко увеличилось, составив на сегодняшний день 116 преступлений. Например, превышение уровня киберпреступности по сравнению с 2008 годом можно классифицировать следующим образом: рост по сравнению с 2008 годом в 2009 году – 50%, 2010 – 66%, 2011 – 30%, в 2012-2013 годах показатели не сильно различаются, 2014 – 33,3%, 2015 – 85,71%, 2016 – 75%, 2017 – 30,46%, в 2018-2019 годах показатели совершения также не сильно различаются (т.е. в эти годы зарегистрировано 13 киберпреступлений), 52% – в 2020 г., в 2021 г. – преступлений не зарегистрировано, 42,5% – в 2022 г. и 49,05% – за первые 6 месяцев 2023 г.)[2].

Следует отметить, что, по данным Всемирного экономического форума (далее ВЭФ), лица, совершающие преступления посредством использования информационно-коммуникационных технологий ИКТ в общем пространстве (в «независимой» форме), представляют один из пяти основных глобальных рисков, угрожающих экономической безопасности, поскольку при наличии и успешном функционировании всех секторов экономики такие лица пред-

[1] Официальный сайт Президента Республики Таджикистан [Электронный ресурс]. – Режим доступа: http://www.president.tj (дата обращения: 29.12.2023).

[2] См.: Официальные статистические данные Информационно-аналитические центр МВД РТ от 25 ноября 2023 года, №14/3-1355.

ставляют опасность. Согласно отчету, ВЭФ, только в 2019 году потери мировой экономики от кибератак составили 2,5 триллиона долларов, а в 2022 году это число выросло до 8 триллионов долларов[3].

В связи с этим, на сегодняшний день в социальных сетях было много ложной рекламы и обмана со стороны мошенников. Некоторые граждане поверили им, потерпев при этом материально-экономический ущерб, связанный с переводом крупных денежных средств, что вызвало озабоченность, поскольку ущерб, нанесенный этим видом преступлений экономике Республики Таджикистан по своей природе очень велик. Например, несколько случаев распространения ложных объявлений в Интернете, которым верят граждане и которые ежедневно фигурируют в социальных сетях – это финансовая поддержка и участие в инвестиционных проектах мошеннических иностранных компаний, таких как «Газпром-инвест», «Алиф-инвест», «Тесла-х» и т. д. относятся к числу тех, которые организованы и управляются обманным путем с целью хищения средств граждан. Оказание финансовой помощи политиками и щедрыми людьми также связано с этим вопросом. Другой случай – наследование денежных средств от дальних родственников, предложение подарков из-за границы в виде «посылки», конечно, направления и виды мошенничества в Интернете увеличиваются, в частности когда поднимается шум о мошенничестве в Интернете и потерянных средствах, создаются новые способы осуществления такого рода вредного для общества поведения, разрабатываются и размещаются на сайтах Интернета новые программы[4]. Только за счет мошенничества в виртуальном пространстве, признанного новым видом киберпреступности, за первое полугодие 2023 года физическим лицам был нанесён материальный ущерб в размере, превышающем 1 млн сомони. Другими видами киберпреступлений, включая незаконный доступ к компьютерной информации и изменение компьютерной информации, в течение 5 прошлых лет юридическим лицам причинен особо крупный материальный ущерб на сумму более 2090377,95 сомони, что в общей сложности составляет 1000750,569 сомони[5]. По статистике Аналитико-информационного центра МВД Республики Таджикистан, первые киберпреступления в Республике Таджикистан были зафиксированы в 2008 году. С тех пор он публиковался в различных формах, в том числе через Интернет-сайты, ИКТ и компьютеры, а интенсивность его публикации через Интернет-сайты фиксировалась в последние пять лет. Например, только за 2022 год Управление по борьбе с организованной преступностью МВД Республики Таджикистан выявило 17 случаев киберпреступ-

[3] См.: Лавров С.В. Глобальные проблемы кибербезопасности и международные инициативы России по борьбе с киберпреступностью / С.В. Лавров // Внешнеэкономические связи. – Октябрь 2020. – С. 6-13.

[4] См.: [Электронный ресурс]. – Режим доступа: https://www.facebook.com/nbt.tj/videos/12526540187 52070/?extid (дата обращения: 29.12.2023).

[5] См.: Официальные статистические данные Информационно-аналитические центр МВД РТ от 25 ноября 2023 года, №14/3-1355; Официальный сайт Генеральный прокуратура Республики Таджикистан [Электронный ресурс]. – Режим доступа: www.prokuratura.tj/ (дата обращения: 01.06.2023).

ности, а также зафиксировало более 500 инцидентов с использованием сети Интернет и информационно-коммуникационных технологий.

В последние годы нормативно-правовая база в сфере противодействия киберпреступности активно развивается на национальном, региональном и международном уровнях. При этом до сих пор не существует единого международно-правового механизма борьбы с киберпреступностью в глобальном масштабе, не выработаны единые условия в этой сфере, что затрудняет сотрудничество государств в этом направлении. Потому что статистика киберпреступлений в странах-участницах СНГ показывает, что в 2020 году количество зарегистрированных преступлений в сфере киберпреступлений выросло в 4 раза: то есть со 125 244 случаев в 2018 году до 536 516 случаев в 2020 году. странах доля уголовных дел, направленных в суд с обвинительным заключением, составляет 18,2% (2019 г. – 23%, 2018 г. – 24,8%) от общего количества зарегистрированных преступлений в этой сфере, 73,6% из которых остались нераскрытыми в 2020 г. (2018 г. – 66,5 %; 2019 г. – 68,4%)[6].

Таким образом, указанные положения обосновывают актуальность темы данного диссертационного исследования.

Степень изученности научной темы. Уголовно-правовые и криминологические вопросы противодействия киберпреступности: теоретические и практические проблемы как с точки зрения теории, так и практики уже многие годы привлекают внимание исследователей и сотрудников правоохранительных органов. Уголовно-правовые вопросы борьбы с киберпреступностью в основном обсуждаются в отечественных и зарубежных научных трудах по праву, в том числе в работах таких авторов как В.А. Абдухамитов[7], Н.Б. Азимзода и З.А. Саидзода[8], Ю.М. Батурин[9], И.Р. Бегишев[10], С.Ю. Битко[11], С.Д. Бражник[12], Л.А. Букалерова[13], В.В. Воробев[14], К.Н. Евдокимов[15],

[6] См.: Сводные отчеты «О состоянии преступности и результатах расследования преступлений» на территории государств-участников СНГ за январь-декабрь 2018 г., 2019 г., 2020 г. // Ф.785 КН.1.; Состояние преступности в государствах-участниках СНГ в 2019 году [Электронный ресурс]. – Режим доступа: https://www.ksgp-cis.ru/about/obzory/sostojanie-prestupnosti-v-2019-godu (дата обращения: 21.04.2023).

[7] См.: Абдухамитов В.А. Борьба с религиозным экстремизмом: уголовно-правовые, криминоло-гические проблемы (на материалах Республики Таджикистан): дис. ... д-ра юрид. наук. – Душанбе, 2016. – 335 с.

[8] См.: Азимзода Н.Б., Саидзода З.А. Таърих ва моҳияти иҷтимой-ҳуқуқии ҷанги иттилоотӣ / Н.Б. Азимзода, З.А. Саидзода // Осори Академияи ВКД Ҷумхурии Тоҷикистон. – 2021. – №4 (52). – С. 84-91.

[9] См.: Батурин Ю.М. Компьютерная преступность и компьютерная безопасность. – М.: Юрид. лит., 1991. – 160 с.

[10] См.: Бегишев И.Р. Понятие и виды преступлений в сфере обращения цифровой информации: дис. ... канд. юрид. наук. – Казань, 2017. – 204 с.

[11] См.: Бытко С.Ю. Некоторые проблемы уголовной ответственности за преступления, совершаемые с использованием компьютерных технологий: дис… канд. юрид. наук. – Саратов, 2002. – 204 с.

[12] См.: Бражник С.Д. Преступления в сфере компьютерной информации: проблемы законодательной техники: дис. ... канд. юрид. наук. – Ижевск, 2002. – 189 с.

[13] См.: Букалерова Л.А. Информационные преступления в сфере государственного и муниципального управления: законотворческие и правоприменительные проблемы: дис. ... д-ра юрид. наук. – М., 2007. – 574 с.

[14] См.: Воробьев В.В. Преступления в сфере компьютерной информации: юридическая характеристика составов и квалификация: дис. ... канд. юрид. наук. – Н. Новгород, 2000. – 201 с.

[15] См.: Евдокимов К.Н. Противодействие компьютерной преступности: теория, законодательство, практика. дис. ... д-ра юрид. наук. –Москва, 2021. – 557 с.

У.В. Зинина[16], П.Н. Кобец[17], В.С. Комиссаров[18], Н.А. Кудратов[19], Ю.И. Ляпунов[20], Д.Г. Малишенко[21], З.Дж. Маджидзода, А.Г. Холикзода и Р.С. Одиназода[22], А.К. Назаров[23], Н.Дж. Назаров[24], С.А. Пашин[25], А.Э. Побегайло[26], Л.Н. Попов[27], М.А. Простосердов[28], Д.В. Пучков[29], Р.Х. Рахимзода[30], Х.С. Сафарзода и Ш.Т. Ахёзода[31], О.М. Сафонов[32], Т.Г. Смирнов[33], М.В. Старичков[34], В.Г. Степанов-Егиянц[35], А.В. Суслопаров[36], Т.Л. Тропина[37], Ф.Р. Шарифзо-

[16] См.: Зинина У.В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве: дис. ... канд. юрид. наук. – М., 2007. – 160 с.

[17] См.: Кобец П.Н. О современных информационных технологиях, используемых экстремистскими и террористическими группировками, и необходимости противодействия киберпреступности / П.Н. Кобец // Вестник развития науки и образования. – 2016. – №6. – С. 4-9.

[18] См.: Российское уголовное право. Особенная часть / Под ред. В.С. Комиссарова. – СПб.: Питер, 2008. – 720 с.

[19] См.: Кудратов Н.А. Уголовно-правовая охрана основ конституционного строя и безопасности государства: проблемы доктрины, правоприменения и совершенствования законодательства: дис. ... д-ра юрид. наук. – Душанбе, 2021. – 540 с.

[20] См.: Ляпунов Ю.И., Максимов В.Ю. Ответственность за компьютерные преступления / Ю.И. Ляпунов, В.Ю. Максимов // Законность. – 1997. – №1. – С. 7-12.

[21] См.: Малышенко Д.Г. Уголовная ответственность за неправомерный доступ к компьютерной информации: дис. ... канд. юрид. наук. – М., 2002. – 166 с.

[22] См.: Мачидзода З.Ҷ., Холиқзода А.Ғ., Одиназода Р.С. Ҷавонон ва амнияти иттилоотӣ (дар масири ҷаҳонишавӣ). – Душанбе, 2019. – 240 с.

[23] См.: Назаров А.Қ., Давлатзода К.Д. Таҳлили муқоисавии ҳуқуқии ҷиноятӣ дар самти мубориза бар зидди ҷиноятҳои компютерӣ дар кишварҳои аъзои ИДМ ва дигар давлатҳои хориҷӣ / А.Қ. Назаров, К.Д. Давлатзода // Паёми Донишгоҳи миллии Тоҷикистон. Бахши илмҳои иҷтимоӣ-иқтисодӣ ва ҷамъиятӣ. – 2022. – №3. – С. 229-236.

[24] См.: Мачидзода Ҷ.З., Назаров Н.Ҷ. Ҷиноятқории муташаккил ва трансмиллӣ. – Душанбе, 2014. – 268 с.

[25] См.: Комментарий к Уголовному кодексу Российской Федерации / Под общ. ред. Ю.И. Скуратова, В.М. Лебедева / Авт. главы С.А. Пашин. – М.: ИНФРА-М: Норма, 2002. – 960 с.

[26] См.: Побегайло А.Э. Борьба с киберпреступностью: учеб. пособие. – М., 2018. – 184 с.

[27] См.: Информационное право: учебник / Л.Л. Попов, Ю.И. Мигачев, С.В. Тихомиров. – М.: Норма: ИНФРА-М, 2010. – 496 с.

[28] См.: Простосердов М.А. Экономические преступления, совершаемые в киберпространстве. – М.: Юрлитинформ, 2017. – 168 с.

[29] См.: Пучков Д.В. Кибертерроризм как новая угроза современного общества / Д.В. Пучков // Виктимология. – 2021. – Т. 8. – №4. – С. 382-390.

[30] См.: Раҳимзода Р.Ҳ. К новым реалиям через уроки и выводы / Р.Ҳ. Раҳимзода // Сотружество. Журнал совета министров внутренних дел СНГ. – 2021. – №1. – С. 4-11.

[31] См.: Сафарзода Ҳ.С., Аҳёзода Ш.Т. Вижагиҳои хосси ҷиноятҳои характери экстремистидошта, ки бо истифодаи ВАО, шабакаҳои алоқаи барқӣ, аз ҷумла Интернет, содир карда мешаванд / Ҳ.С. Сафарзода, Ш.Т. Аҳёзода // Осори Академияи ВКД Ҷумҳурии Тоҷикистон. – 2021. – №4 (52). – С. 92-100.

[32] См.: Сафонов О.М. Уголовно-правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и правоприменительной практики, перспективы совершенствования: дис. ... канд. юрид. наук. – М., 2015. – 222 с.

[33] См.: Смирнова Т.Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации: дис. ... канд. юрид. наук. – М., 1998. – 161 с.

[34] См.: Старичков М.В. Умышленные преступления в сфере компьютерной информации: уголовно-правовая и криминологическая характеристики: автореф. дис. ... канд. юрид. наук. – Иркутск, 2006. – 29 с.

[35] См.: Степанов-Егиянц В.Г. Методологическое и законодательное обеспечение безопасности компьютерной информации в Российской Федерации: уголовно-правовой аспект: дис. ... д-ра юрид. наук. – М., 2015. – 389 с.

[36] См.: Суслопаров А.В. Информационные преступления: дис. ... канд. юрид. наук. – Красноярск, 2008. – 249 с.

[37] См.: Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. ... канд. юрид. наук. – Владивосток, 2005. – 234 с.

да[38], Р.Ш. Шарофзода[39], В.В. Челноков[40] и других. В рамках диссертационных исследований указанным ученым удалось изучить различные аспекты этих опасных для общества действий в виртуальном пространстве.

По криминологическим вопросам киберпреступлений к научным трудам относятся работы таких ученых как А.П. Алексеев[41], С.Э. Бахриддинов[42], А.А. Жмихов[43], В.Э. Керимов[44], Т.П. Кесареева[45], В.В. Крилова[46], В.С. Овчинского[47], А.Л. Осипенко[48], А.Э. Побегайло[49] и других авторов.

Работы указанных ученых позволяют получить определенные сведения (сформировать представления) о сущности и содержании киберпреступности, но, к сожалению, практически не затрагивают современные проблемы (киберзапугивание информационной безопасности) и уголовное законодательство Республики Таджикистан в этой области.

Их работы посвящены реальной ситуации информационного пространства мира, практическому опыту сотрудников оперативных параграфений борющихся субъектов с киберпреступностью и ее опасностью для общественности, эти работы имеют большое значение для развития уголовно-правовой доктрины в противодействии киберпреступности, поскольку в глобальном масштабе до сих пор не существует единого международного правового механизма противодействия киберпреступности в этих областях, в связи с чем, этот фактор затрудняет сотрудничество государств в этом направлении.

Конечно, в этом направлении много неисследованных аспектов, в связи с этим, необходимо проведение подробного исследования уголовно-правовых и криминологических вопросов обеспечения безопасности информации от кибе-

---

[38] См.: Шарифзода Ф.Р. Теоретико-правовые основы организации деятельности органов внутренних дел Республики Таджикистан в системе обеспечения национальной безопасности государства: монография / Под ред. д.ю.н., профессора, Заслуженного юриста Российской Федерации Анатолий Михайловича Кононова. – Душанбе: ЭР-граф, 2023. – 267 с.

[39] См.: Шарофзода Р.Ш., Шокиров Ғ.А. Заминаҳои илмӣ-ҳуқуқии иттилоотонӣ ва бунёди чомеаи иттилоотӣ дар Ҷумҳурии Тоҷикистон / Р.Ш. Шарофзода, Ғ.А. Шокиров // Осори Академияи ВКД Ҷумҳурии Тоҷикистон. – 2021. – №4 (52). – С. 110-120.

[40] См.: Челноков В.В. Компьютерная информация как предмет преступления в отечественном уголовном праве: дис. ... канд. юрид. наук. – Екатеринбург, 2013. – 226 с.

[41] См.: Алексеева А.П. Киберпреступность: основные черты и формы проявления / А.П. Алексеева, О.Н. Ничуговская // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. – 2017. – №1. – С. 27-34.

[42] См.: Бахриддинов С.Э. Криминология: китоби дарсӣ. Қисми умумӣ. – Душанбе, 2013. – 187 с.

[43] См.: Жмыхов А.А. Компьютерная преступность за рубежом и ее предупреждение: дис. ... канд. юрид. наук. – М., 2003. – 178 с.

[44] См.: Керимов В.Э., Керимов В.В. Профилактика и предупреждение преступлений в сфере компьютерной информации / В.Э. Керимов, В.В. Керимов // Черные дыры в российском законодательстве. – 2002. – №1. – С. 503-513.

[45] См.: Кесареева Т.П. Криминологическая характеристика и проблемы предупреждения преступности в российском сегменте сети Интернет: автореф. дис... канд. юрид. наук. – М., 2002. – 25 с.

[46] См.: Крылов В.В. Криминалистические проблемы оценки преступлений в сфере компьютерной информации / В.В. Крылов // Уголовное право. – 1998. – №3. – С. 83-91.

[47] См.: Овчинский В.С. Криминология цифрового мира: учебник для магистратуры. – М.: Норма: ИНФРА-М, 2018. – 352 с.

[48] См.: Осипенко А.Л. Организованная преступная деятельность в киберпространстве: тенденции и противодействие / А.Л. Осипенко // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2017. – №4 (40). – С. 181-188.

[49] См.: Побегайло А.Э. Киберпреступность: учеб. пособие (для бакалавров). – М., 2014. – 96 с.

ратак. В условиях глобализации необходимо задуматься о понятии киберпреступности и ее опасности для общества, классификации киберпреступлений, международного сотрудничества в борьбе с киберпреступлениями.

Связь исследования с программами либо научной тематикой. Диссертационное исследование выполнено в рамках «Государственной программы по борьбе с преступностью в Республике Таджикистан на 2021-2030 годы» и научно-исследовательской работы на базе кафедре криминалистики и судебно-экспертной деятельности, кафедры уголовного права, и противодействия коррупции юридического факультета Таджикского национального университета.

ОБЩАЯ ХАРАКТЕРИСТИКА ИССЛЕДОВАНИЯ

Цель исследования. Целью диссертационного исследования является изучение уголовно-уголовных вопросов киберпреступности, ее криминологических аспектов, разработка теоретических и практических основ борьбы с киберпреступностью в Республике Таджикистан в условиях глобализации, стремительного развития информационно-коммуникационных технологий, угрозы и опасности кибератак для информационной безопасности страны, а также предложить новации по повышению эффективности уголовно-правового и криминологического регулирования борьбы с киберпреступностью.

Задачи исследования. Для достижения этих целей необходимо решить следующие задачи:

– изучить и выявить эволюцию компьютерных вирусов как основного фактора формирования киберпреступлений.

– анализ и представление понятия киберпреступлений;

– определение перечня киберпреступлений и основы их классификации;

– порядок установления международного сотрудничества в борьбе с киберпреступностью;

– изучение дифференциации уголовной ответственности за киберпреступления по уголовному законодательству зарубежных стран;

– научно-практический анализ объективных признаков преступлений против сетей Интернет и их вспомогательного оборудования (вредоносные программы, DoS-атаки);

– рассмотрение и выявление субъективных признаков преступлений против сетей Интернет и их вспомогательного оборудования (вредоносные программы, DoS-атаки);

– изучение и выявление объективных признаков преступлений, совершенных с использованием различных технических средств (фишинговое письмо, кибersталкинг, кража онлайн-личности);

– анализ правовой практики субъективных признаков преступлений, совершенных с использованием различных технических средств (фишинговое письмо, кибersталкинг, кража онлайн-личности);

– анализ состояние, структура, динамика киберпреступности;

– обзор криминологических особенностей личности киберпреступника;
– анализ, предупреждение и профилактика киберпреступлений.

Объект исследования. В качестве объекта исследования выступает комплекс общественных отношений, возникающих в связи с совершением киберпреступлений.

Предмет исследования – это нормы уголовного законодательства зарубежных стран и Республики Таджикистан, положения иных нормативных правовых актов, направленных на борьбу с киберпреступностью, материалы уголовных дел из архивов, рассмотренных судами Республики Таджикистан или следственными органами.

Этап, место и период исследования (историческое рамки исследования). Местом исследования является кафедра криминалистики и судебно-экспертной деятельности юридического факультета Таджикского национального университета. Период исследования охватывает 2019-2024 годы и состоит из двух этапов.

На первом этапе (2019-2020 гг.) были систематизированы научно-информационные источники, связанные с предметом исследования, утверждены Ученым советом.

На втором этапе (2020-2024 годы) были выполнены поставленные цели и задачи. По теме исследования были опубликованы научные статьи и подготовлен диссертация. Подготовлен проект Закона Республики Таджикистан «О кибербезопасности».

Теоретические основы исследования. Теоретическую основу исследования составили Послания Основателя мира и национального единства – Лидера нации, Президента РТ, уважаемого Эмомали Рахмона и сборник теоретических и практических работ по основным проблемам уголовно-правовой доктрины. В зависимости от исследуемой темы были изучены труды отечественных и зарубежных ученых, в том числе таких авторов как В.Б. Веховим, А.Г. Волеводзом, Ю.В. Гаврилиним, Л.Д. Галиакбаров, А.А. Гаухман, Т.А. Герсензон, В.А. Голубевим, А.И. Долгова, Г.А. Есаков, А.М. Жодзишский, Р.В. Жубрин, О.С. Капинус, М.И. Ковалевим, И.Я. Козаченко, В.Е. Козловим, В.С. Комиссаров, А.И. Коробеевим, С.М. Кочои, В.Н. Кудрявцевим, Н.Ф. Кузнецовой, Б.А. Куринов, В.Д. Курушин, А.Н. Ларков, В.Н. Лопатин, Н.А. Лопашенко, В.В. Лунеев, Ю.И. Ляпуновим, З.Дж. Маджидзода, А.К. Назаров, А.В. Наумовим, Б.С. Никифоров, С.И. Никулиним, В.А. Номоконов, К.В. Ображиев, В.С. Овчинский, А.Л. Осипенко, А.В. Павлинов, С.В. Пархоменко, А.А. Пионтковский, С.В. Полубинской, А.И. Рарог, Т.В. Раскина, И.М. Рассолов, С.В. Расторопов, Р.Х. Рахимзода, В.С. Савелева, А.И. Сафарзода, Д.А. Соколов, Н.С. Таганцев, А.Н. Трайнин, А.Г. Холикзода, А.И. Чучаев, Т.Ш. Шарипов, Ф.Р. Шарифзода, Р.Ш. Шарофзода, П.С. Яни, которые имеют большое теоретическое значение.

Эти ученые создали подходящую теоретическую основу для анализа проблем совершения киберпреступлений, идентификации киберпреступника

(хакера), предотвращения киберпреступлений, классификации киберпреступлений в сфере преступности против информационной безопасности.

Кроме того, теоретической основой исследования являются научные публикации электронных интернет-ресурсов, посвященные уголовно-правовым и криминологическим вопросам борьбы с киберпреступностью.

Методологические основы исследования. В ходе исследования были использованы диалектические методы, а также для решения поставленных задач использовались институциональные, формально-правовые, формально-логические, сравнительно-правовые, статистические и другие общие и специальные научные методы, разработанные наукой и проверенные на практике. Общенаучные методы позволили изучить роль информационно-коммуникационных технологий, в развитии общества и их влияние на современное общество, и то какое послание имеет их беспрепятственное использование в условиях глобализации. Методология, используемая в исследовании, создала условия для того, чтобы она была исчерпывающей и определяла появление новых явлений и субподрядов, а также выявляла новые тенденции международного сотрудничества в противодействии киберпреступности и предлагала новые идеи для эффективного их осуществления на практике.

Эмпирические предпосылки. В процессе исследования был изучен опыт правоохранительных органов Республики Таджикистан в области противодействия киберпреступности, в том числе Генеральной прокуратуры Республики Таджикистан, изучено более 116 случаев из архивов Верховного Суда Республики Таджикистан, статистических данных Главного аналитико-информационного центра Министерства внутренних дел Республики Таджикистан, Управления по борьбе с организованными преступлениями Республики Таджикистан, Министерства юстиции Республики Таджикистан, практики международных организаций, в том числе ООН, Международного союза телекоммуникаций, Интерпола, Европола, МВД Республики Таджикистан, ШОС и Организация Договора о коллективной безопасности.

Научная новизна исследования. Данная работа является первым отечественным диссертационным исследованием, охватывающим теоретические и практические проблемы уголовно-правовых и криминологических вопросов противодействия киберпреступности. Следует отметить, что ранее на уровне монографических и диссертационных исследований подробно не анализировались уголовно-правовые и криминологические вопросы противодействия киберпреступности.

Положения, выносимые на защиту. На защиту представлены следующие научные положения, представляющие новизну диссертации:

1. Киберпреступность – совокупность преступлений, направленных на использование программно-технических средств обучения и ИКТ в общем пространстве с целью незаконного получения, изменения информации, уничтожения или отмены информационных систем и ресурсов, направлен-

ных на причинение вреда конституционным правам и свободам человека и гражданина, государственной и общественной безопасности или имущественным отношениям.

2. С учетом того, что человечество в начале XXI века столкнулось с новыми угрозами и опасностями информационного мира, обеспечение информационной безопасности от кибератак, в том числе актуальной задачей современного государства (кибератаки, незаконное проникновение в информационные системы, распространение вредоносных программ и компьютерных вирусов) серьезно сказывается на национальной безопасности государства.

3. Международные инициативы Республики Таджикистан по обеспечению информационной безопасности от кибератак и противодействию киберпреступности включают в себя следующие этапы:

– первый этап, в 1992 году в городе Ташкенте Республики Узбекистан было подписано «Соглашение о предоставлении цифровых средств и информационной безопасности» между государствами-членами Союза Независимых Государств;

– второй этап состоялся 1 июня 2001 года в городе Минске Белорусской Республики, подписав «Соглашение о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации».

4. В рамках ОДКБ создан «Центр по борьбе с киберпреступностью» как специализированный орган. Целью его создания является сбор и обработка данных о киберпреступлениях, проведение экспертной оценки киберугроз, разработка и внедрение передовых методов борьбы с киберпреступностью, предупреждение и расследование, обучение новых кадров, продвижение правоохранительных органов, повышение уровня безопасности информационного пространства от кибератак в регионе и мире, а также налаживание разрешения вопроса их прозрачного сотрудничества в направлении организационного обеспечения борьбы с киберпреступностью.

5. В целях предупреждения и предотвращения киберпреступлений в Республике Таджикистан Единый коммутационный центр Службы связи Правительства Республики Таджикистан, Генеральной прокуратуры Республики Таджикистан и Министерства внутренних дел Республики Таджикистан в условиях глобализации, а также быстрой компьютеризации всех жизненно важных государственных ведомств с целью обеспечения безопасности информации от кибератак в стране, доступа к веб-сайтам и другим информационным ресурсам, включая веб-сайты и интернет-программы, которые связаны с возможностью распространения любой информации, направленной на нарушение основ конституционного строя, личной, общественной и государственной безопасности, информации об ограничении прав и свобод человека и гражданина, разжигании религиозной ненависти и вражды, религиозного или национального конфликта, расовой, региональной дискриминации, способы изготовления и продвижения наркотических средств, взрывчатых и других отравляющих веществ,

направленных на совершение преступлений и административных правонарушений, экстремистского и террористического характера, порнографии, в том числе детской порнографии, а также ограничение распространения, предоставление любой информации, которая запрещена нормативно-правовыми актами Республики Таджикистан.

6. Киберпреступность в целом может быть классифицирована по следующим основаниям:

а) в зависимости от объекта преступного посягательства: нарушение прав и интересов владельцев компьютерной информации; посягательство на права и интересы владельцев носителей информации;

б) по характеру вреда, причиняемого компьютерной информации: вредоносные программы, изменяющие, уничтожающие, блокирующие, выводящие из строя, копирующие компьютерную информацию;

в) в зависимости от способов совершения преступления: отправка писем путем обмана; их совершение через интернет.

7. В зарубежных и постсоветских государствах установлено различное правовое регулирование уголовной ответственности за киберпреступность:

– различные объекты преступного посягательства в области киберпреступлений определены в уголовном законодательстве постсоветских государств и зарубежных стран. Помимо отношений в области безопасного обращения с компьютерной информацией, они включают также конституционные права и свободы человека и гражданина (например, свобода и всеобщий мир во французском и немецком уголовном законодательстве), национальную безопасность и нормальную экономическую деятельность (в уголовном законодательстве США), а также общественный порядок и общественная безопасность (в уголовном законодательстве Республики Казахстан). Это свидетельствует о том, что киберпреступления влияют не только на отдельные компьютерные системы или информацию, но и на различные аспекты общественной жизни и общественные ценности;

– установлено, что в уголовном законодательстве зарубежных стран субъекты преступлений против кибербезопасности делятся на две группы: государства, где субъектом этого преступления является только вменяемое физическое лицо, достигшее указанного возраста, и в отдельных случаях действует специальный субъект (Республики Кыргызстан, Узбекистан, Казахстан и др.); государства, признающие субъектами этих преступлений наравне с физическими лицами юридические лица, (Дания, Латвия, Литва, Молдова, Франция, Швеция, Эстония и др.);

– уголовное законодательство зарубежных стран содержат в себе различные положения о действиях, квалифицируемых (признаваемых) в качестве киберпреступлений. В группе государств (например, Китайская Республика) неисполнение специальными субъектами решений субъектов борьбы с киберпреступностью о блокировке соответствующих интернет-ресурсов и удалении запрещенной информации рассматривается в качестве виртуально-

го содействия совершению киберпреступлений. За использование Интернет-ресурсов с целью распространения информации о способах совершения преступления, предусмотрена уголовная ответственность (ст. 285А, 286А, 287А, 287Б). В некоторых случаях государства устанавливают уголовную ответственность за преступления, совершаемые с использованием ИКТ, в том числе интернет-мошенников. (Республика Молдова, Российская Федерация, Великобритания, Испания, Бельгия, Дания, Эстония и др.).

8. В качестве объектов преступлений против сетей интернет и поддерживающего их оборудования выступают**:** информационная безопасность, права и интересы субъектов правоотношений, а также различные материальные и нематериальные ценности. Преступления в данной сфере могут привести к нанесению ущерба жизни, здоровью, имуществу и другим интересам людей, а также нарушению законом защищаемых прав и свобод. Необходимо принимать соответствующие меры для защиты информационной безопасности и пресечения преступной деятельности в данной области (физических и юридических лиц и органов местного самоуправления).

9. Обосновывается необходимость классификации объектов преступлений против сетей интернет на следующие виды**:**

– видовой объект преступлений против сетей Интернет и поддерживающего их оборудования (вредоносные программы и DoS-атаки), важные охраняемые уголовным законодательством общественные отношения в области безопасности разработки, использования и распространения компьютерной информации, информационных ресурсов, информационных систем и ИКТ, права и интересы физических и юридических лиц, общества и государства по использованию системы автоматической обработки данных;

– непосредственный объект преступлений против сетей Интернет и их вспомогательного оборудования в зависимости от его характера как вида киберпреступности включает в себя два объекта:

а) основными объектами данных преступлений являются общественные отношения, непосредственно затрагивающие права и законные интересы владельцев компьютерной информации и регуляторов информационных систем в сфере разработки, обработки, владения, распространения, представления и использования компьютерной информации, компьютерных систем, компьютерных сетей, информационных систем и безопасной эксплуатации, и информационно-коммуникационных сетей;

б) дополнительными объектами данных преступлений являются общественные отношения, которые регулируются правовыми нормами и обеспечивают права и законные интересы личности, общества и государства.

10. Из рассмотрения и анализа объекта преступлений против сетей интеренет и их вспомогательного оборудования вытекает, что общественно значимые действия (вредоносные программы, DoS-атаки) наносят ущерб не только информационной безопасности, но и различным общественным отношениям, создавая угрозу причинения такого вреда. Отече-

ственным уголовным законодательством данная категория этого преступления предусмотрена в главе 28 «Преступления против информационной безопасности», а учитывая иные общественные отношения, включенные в данную главу (кибертерроризм, киберэкстремизм, киберсталкинг, фишинг и т.п.), считаем целесообразным ввести в Уголовный кодекс Республики Таджикистан новый раздел под названием «Преступления против кибербезопасности».

11. В новый раздел «Преступления против кибербезопасности» входят следующие главы: преступления против интернет-сетей и их вспомогательного оборудования (деструктивные киберпреступности); преступления, совершаемые с использованием интернет-сети и электронных информационных ресурсов (социальные сети мессенджеры и другие ресурсы); преступления, совершаемые с использованием различных технических средств; преступления, угрожающие жизни и здоровью; преступления, нарушающие конфиденциальность информации включая незаконный доступ к компьютерам или компьютерным системам без ущерба для информации.

12. Субъектом преступлений, направленных против сетей Интернет и поддерживающего их оборудования (вредоносные программы, DoS-атаки), может быть вменяемое физические лицо и исполнитель (т.е. общий субъект преступления), достигший на момент совершения преступления 14-летнего возраста. Люди в возрасте 14-19 лет в наше время являются пользователями системы Интернет и владеют компьютерными устройствами (мобильными телефонами, смартфонами, ноутбуками, планшетами и т.д.) и обладают знаниями, умениями и необходимыми навыками для работы с ИКТ. Следовательно, у них имеется теоретическая и практическая возможность совершить объективную часть рассматриваемого преступления. Необходимо добавить к части 2 статьи 23 Уголовного кодекса Республики Таджикистан (по возрасту уголовной ответственности) состав преступлений, предусмотренных статьями 300 и 303 УК РТ, а дополнительная уголовная ответственность за такие преступления должна быть установлена с 14 лет.

13. Объективная сторона преступлений, совершаемых с применением различных технических средств, включает совокупность признаков, указывающих на поведение лица, связанное с незаконным сбором информации о другом лице, распространением информации в широком кругу публично или в средствах массовой информации, отображение информации, а также рассылка мошеннических электронных писем при использовании сети Интернет, что наносит ущерб правам и законным интересам потерпевшего.

Предложения по совершенствованию законодательства:

14. Автором разработан проект Закона Республики Таджикистан «О кибербезопасности», в котором для обеспечения информационной безопасности от кибератак предусмотрены общие положения о действиях закона, государственном регулировании кибербезопасности, права и обязанности государственных органов и государственных организаций по обеспечению ки-

бербезопасности, обеспечению кибербезопасности, инцидентов кибербезопасности, объектов критической информационной инфраструктуры, поддержке и развитию обеспечения кибербезопасности, международного сотрудничества в области кибербезопасности и других важных направлений правового регулирования.

15. В целях совершенствования уголовного законодательства и усиления норм главы 28 УК РК считаем необходимым внесение изменений и дополнений в уголовное законодательство. В частности, в следующие статьи:

Статья 298 (1) Получение персональных электронных данных путем мошенничества или иных способов незаконного доступа к данным в корыстных целях

1. Получение персональных электронных данных через сеть Интернет путем мошенничества или иных способов незаконного доступа к данным с целью использования их в личных целях, наказывается-

на срок до … лет.

2. То же деяния, если вызвало крупный ущерб, наказывается на срок до … лет

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой, или лицом, злоупотребляющим своим служебным положением, наказывается на срок до … лет

4. Деяния, предусмотренные частями первой, второй и третьей настоящей статьи, если они повлекли тяжкие последствия или привели к риску их возникновения, наказывается на срок до … лет

16. Считаем необходимым добавить к статье 300 Уголовного кодекса РТ, пункт 2 в следующей редакции:

«Те же действия,

в) совершенные с целью хулиганства;

г) в целях запугать население или повлиять на принятие решений государственными органами и (или) местным самоуправлением;

д) в целях воспрепятствования нормальному функционированию средств массовой информации, органов государственной власти и (или) местного самоуправления, государственных учреждений.

17. В главу 28 УК РТ предлагается внести новые статьи (статьи 300 (1) и 300 (2)) следующего содержания:

Статья 300 (1) Компьютерная атака DoS

1) DoS-атака на компьютер, целенаправленное воздействие на компьютерную систему или сеть с использованием вредоносных программ, направленное на нарушение ее работы, в результате чего произошло лишение пользователей возможности доступа к запрошенному электронному ресурсу, -

наказывается сроком до … лет

Статья 301 (2). Незаконное распространение электронных сообщений в публичной форме

1) Незаконное массовое распространение нежелательных сообщений, – рассылка массовых электронных писем экстремистского, террористического пропагандистского характера через сеть Интернет или с использованием телефона, факса, радио, мобильной связи, в том числе с использованием средств подбора и (или) дозвона абоненту, -

наказывается сроком до … лет

2) То же деяние, совершенное группой лиц по предварительному сговору, -

наказывается сроком до … лет

3) деяния, предусмотренные частями первой или второй настоящей статьи, совершенные организованной группой или с использованием служебного положения, -

наказывается сроком до … лет

18. В этих целях целесообразно дополнить часть 3 статьи 301 УК отдельными пунктами следующего содержания:

д) привести к уничтожению или блокировке информации;

е) совершенные лицом, использующим свое служебное положение, а также лицом, имеющим доступ к компьютерной системе или сети.

В то же время, с учетом охраны общественного порядка и этических и культурных ценностей, статья 301 (3) должна быть включена в УК РТ в следующем содержании:

Статья 301 (3). Разработка, публикация и распространение информации с использованием сети интернет и любых средств информационно-телекоммуникационных сетей

1) Разработка, опубликование и распространение с использованием сети Интернет и любых средств информационных и телекоммуникационных сетей информации, влекущей нарушение общественного порядка, моральных и культурных ценностей, -

наказывается сроком до … лет

19. Обоснование вывода автора с учетом анализа уголовного законодательства зарубежных и постсоветских стран поставило вопрос о необходимости внесения изменений в часть 2 статьи 302 УК РТ:

2) совершение тех же действий, если на территории Республики Таджикистан производится ввод, подготовка, распространение и применение различных видов оборудования и программ, используемых для преобразования идентификационных данных, -

наказывается сроком до … лет

20. Предлагается представить статью 303 Уголовного кодекса Республики Таджикистан в следующей редакции:

Статья 303. Незаконная разработка, использование или распространение вредоносных компьютерных программ

1) Разработка компьютерных программ, внесение изменений в существующую программу с целью незаконного уничтожения, блокирования, мо-

дификации, копирования, использования информации, хранящейся на электронных носителях, хранимой в информационной системе или передаваемой по сетям телекоммуникаций, нарушения эксплуатации компьютера, абонентского устройства, программы для ЭВМ, информационной системы или сети телекоммуникаций, а равно умышленное использование и (или) распространение таких программ, -

наказывается на срок до … лет

2) Те же действия, если они совершены с причинением крупного вреда гражданам, -

наказывается сроком до … лет

3) Деяния, предусмотренные частями первой или второй настоящей статьи, если они совершены в крупном размере, -

наказывается на срок до … лет

4) Если деяния, предусмотренные частями первой и второй настоящей статьи, совершены с использованием служебного положения,-

наказывается сроком до … лет.

Теоретическая и практическая значимость исследования. Теоретическая и практическая значимость исследования выражается в том, что теоретические выводы, полученные в результате диссертационного исследования, могут быть использованы при дальнейшем изучении теоретических и практических вопросов киберпреступности в Республике Таджикистан и других зарубежных странах. Результаты исследования могут быть использованы в деятельности законодательных и правоохранительных органов (КГБ РТ, МВД РТ, Прокуратуры РТ, Министерства юстиции РТ) и судов. Кроме того, результаты исследования целесообразно использовать для совершенствования деятельности правоохранительных органов в направлении обеспечения информационной безопасности от кибератак в условиях глобализации. Материал диссертационного исследования может быть полезен в образовательной деятельности при преподавании учебных дисциплин «Уголовное право», «Уголовное исполнительное право» и «Криминология», одновременно для проведения семинаров, конференций и научных «круглых столов» и практической работы.

Степень достоверности результатов. Опубликованные работы автора признаны преподавателями учебных заведений и правоохранительными органами страны, в том числе Академией МВД Республики Таджикистан, юридическим факультетом Таджикского национального университета, Российско-Таджикским (Славянского) университетом, Национальным законодательным центром при Президенте Республики Таджикистан, отделом по борьбе с киберпреступностью Генеральной прокуратуры Республики Таджикистан и отделом компьютерной техники и видео-фоноскопии Республиканского центра судебной и криминалистической экспертизы Министерства юстиции Республики Таджикистан, использовать при чтении лекций и проведении семинаров (практикумов) со студентами, аспирантами и в процессе повышения квалификации сотрудников правоохранительных органов.

Соответствие диссертации паспорту научной специальности. Диссертационные исследованная соответствует паспорту научной специальности 12.00.08 – Уголовное право и криминология; уголовно-исполнительное право, утвержденного Высшей аттестационной комиссией при Президенте Республики Таджикистан[50].

Личный вклад соискателя ученой степени в исследование проявляется в том, что диссертационное исследование было проведено непосредственно автором, в рамках исследования были объяснены основные понятия, раскрыты новые тенденции, выявлены новые явления международного сотрудничества в противодействии киберпреступности, показаны пути решения актуальных проблем, лежащих в этом направлении в рамках научных положений, представлены выводы и предложения в научных публикациях автора по тематике исследования диссертации. Также, в зависимости от исследуемого вопроса, заявитель принял участие в нескольких научно-практических мероприятиях различного уровня. В целях совершенствования теоретических знаний и повышения профессионального мастерства сотрудников прокуратуры с 22 по 31 августа 2022 года в трех регионах при участии 68 городских и районных прокуроров и приравненных к ним прокуроров города Душанбе, Согдийской и Хатлонской областей, была проведена встреча по предоставлению информации о результатах исследования, необходимых юридических выводах и существующих проблемах и недостатках, выявленных на основе следственно-судебного опыта, использования современных технических средств, уголовно-правовых и криминологических вопросов борьбы с киберпреступлениями, процедурами и методами проведения расследований данного вида рассматриваемых преступлений[51]. Исследователь также является автором множества научных и учебных работ по избранной теме.

Апробация и применение результатов диссертации. Диссертация выполнена на кафедре криминалистики и судебно-экспертной деятельности юридического факультета Таджикского национального университета, несколько раз обсуждалась на его заседаниях, после чего была рекомендована к защите в диссертационном совете 6D.KOA-019. Отдельные результаты диссертационного исследования были представлены на ежегодных республиканских научно-теоретических (практических) конференциях преподавателей (профессорско-преподавательского состава) и сотрудников ТНУ(2017-2023 годы), а также выводы и предложения были апробированы в форме доклада на следующих международных и республиканских конференциях:

а) международные:

– Международная научно-практическая конференция на тему: «Права человека: вчера и сегодня» – доклад на тему: «Проблемы борьбы с компью-

[50] См.: Решение Президиума Высшей аттестационной комиссии при Президенте Республики Таджикистан от 30 сентября 2021 года, №7 // Бюллетень Высшей аттестационной комиссии при Президенте Республики Таджикистан. – 2022. – №1-2 (21-22). – С. 231, 292.

[51] См.: Письмо Генерального прокурора Республики Таджикистан от 11.08.2022, №32/3-145.

терной преступностью как специфической формой киберпреступности» (Душанбе, ТНУ, 9 декабря 2022 г.);

– Международная конференция на тему: «Наука и образование: тенденции развития в информационном обществе», посвященная «75-летию Таджикского национального университета» – доклад на тему: «Международные инициативы Республики Таджикистан в обеспечении информационной безопасности от кибератак» (Душанбе, ТНУ, 20-21 октября 2023 г.);

– Международная научно-практическая конференция на тему: «Таджики в зеркале истории», посвященная 115-летию академика Бабаджана Гафурова – доклад на тему: «Киберугрозы: мошенничество в виртуальном пространстве» (Душанбе, Филиал МГУ имени Михаила Ломоносова в г. Душанбе, 27 октября 2023 г.);

– Международная научно-практическая конференция на тему: «25-летие Уголовного Кодекса Республики Таджикистан: ситуация и перспективы» – доклад на тему: «Международные организации как субъекты борьбы с киберпреступностью» (Душанбе, Академия МВД РТ, 26 мая 2023 г.);

– Международная научно-практическая конференция на тему: «Защита прав человека и проблема борьбы с коррупцией в современном мире: концепции, реальность и перспективы» – доклад на тему: «Интернет как средство совершения кибер-сталкинга» (Душанбе, Академия государственного управления при Президенте Республики Таджикистан, 1-2 декабря 2023 г.);

– Международная научно-теоретическая конференция на тему: «Теоретические вопросы формирования культуры прав человека в Таджикистане» – доклад на тему: «Анализ практического опыта уполномоченных государственных органов и их международного сотрудничества в направлении обеспечения кибербезопасности» (Душанбе, ТНУ, 9 декабря 2023 г.);

б) республиканские:

– Республиканская научно-практическая конференция на тему: «Современная криминалистика» – доклад на тему: «Роль искусственного интеллекта в процессе оперативно-розыскной деятельности». (Душанбе, Академия МВД Республики Таджикистан, 31 декабря 2021 г.);

– Республиканская научно-практическая конференция на тему: «Оперативно-розыскная политика обеспечения безопасности Республики Таджикистан» – доклад на тему: «Уголовно-правовое исследование понятия киберпреступности» (Душанбе, Академия МВД Республики Таджикистан, 4 октября 2022 г.);

– Республиканская научно-теоретическая конференция на тему: «Развитие правоохранительной деятельности в Республике Таджикистан» – доклад на тему: «Роль правоохранительных органов в борьбе с киберпреступностью» (Душанбе, ТНУ, 6 октября 2022 г.);

– Республиканская научно-теоретическая конференция на тему: «Роль Конституции в реализации стратегических целей государства» –

доклад на тему: «Киберпреступления: угрозы XXI века» (Душанбе, ТНУ, 1 ноября 2022 г.);

– Республиканская научно-теоретическая конференция на тему: «Конституция Республики Таджикистан и национальная правовая система» – доклад на тему: «Киберпреступность как угроза общественной безопасности» (Душанбе, Академия МВД Республики Таджикистан, 3 ноября 2022 г.);

– Республиканская научно-практическая конференция на тему: «Проблемы земельного законодательства Республики Таджикистан в современности» – доклад на тему: «Вредоносные программы как средство совершения киберпреступлений: их определение и виды» (Душанбе, ТНУ, 13 октября 2023 г.);

– Республиканская научно-практическая конференция на тему: «Противодействие торговле людьми: проблемы и соображения» – доклад на тему: «Интернет и социальные сети: средство совершения торговли людьми» (Душанбе, «Национальная библиотека Таджикистана», 26 октября 2023 г.);

– Республиканская научно-теоретическая конференция на тему: «Актуальные вопросы совершенствования Конституции Республики Таджикистан в современных условиях» – доклад на тему: «Хакер: его криминологическая характеристика» (Душанбе, ТНУ, 1 ноября 2023 г.).

Отдельные положения диссертации были использованы автором во время чтения лекций по учебной дисциплине «Основы расследования киберпреступлений» (для студентов по специальности «судебная экспертиза») на юридическом факультете ТНУ. Кроме того, результаты исследования были использованы в законодательной деятельности Маджлиси милли Маджлиси Оли РТ, деятельности отдела по борьбе с киберпреступностью Генеральной прокуратуры Республики Таджикистан, отдела компьютерной техники и видео-фоноскопии Республиканского центра судебной и криминалистической экспертизы Министерства юстиции Республики Таджикистан.

Публикации по теме диссертации. По теме диссертации автором было опубликовано 28 научных статей, в том числе 20 статей в изданиях, рецензируемых Высшей аттестационной комиссии при Президенте РТ и 8 статей в других изданиях на таджикском и русском языках. Иследователь также является автором 1 учебника и 1 учебного пособия, содержание которых связано с предметом диссертации. Таким образом, общий объем публикаций заявителя составляет более 85 печатных листов.

Структура и объем диссертации соответствует предметом и объектом, целями и задачами данного исследования. Диссертация состоит из перечня сокращений и (или) условных обозначений, введения, пяти глав, пятнадцати параграфов, заключения, рекомендации по практическому использованию результатов исследования, список литературы (источников) и перечень научных публикаций соискателя ученой степени. Объем диссертации составляет 480 страниц.

ОСНОВНЫЕ ЧАСТИ ИССЛЕДОВАНИЯ (КРАТКОЕ ИЗЛОЖЕНИЕ)

В **введении** обоснована актуальность темы диссертационного исследования, показана степень ее научной обработки, определены цели и задачи диссертационной работы, представлены объект и предмет, методологические и экспериментальные основы исследования, теоретическая и практическая значимость исследования и основные элементы новизны, представляемые к защите.

В первой главе диссертации – **«Теоретические проблемы противодействия киберпреступности»** рассматриваются вопросы разработки компьютерных вирусов как основного фактора формирования киберпреступности, понятия киберпреступности и классификации киберпреступности.

В первом параграфе первой главы – **«Эволюция компьютерных вирусов как основной фактор формирования киберпреступлений»** диссертации упоминается, что в современном мире актуализируются вопросы обеспечения информационной безопасности от кибератак, в том числе регулирования киберпреступности в этой жизненно важной области посредством уголовного законодательства считаются важнейшими вопросами. Современное развитие информационных технологий и все более широкий доступ к компьютерной технике привели к возможности использования их не только в научных, исследовательских и образовательных целях, но и во всех сферах общественной жизни. В диссертации упоминается, что первый этап появления компьютерных вирусов как средства совершения киберпреступлений начался с обнаружения вируса Creeper (1960-1970 гг.) в американской военной компьютерной сети ARPANET (ИНТЕРНЕТ). Для удаления этого вируса была изобретена первая антивирусная программа Reeper. Назначение вируса ARPANET (INTERNET) заключалось в том, чтобы обнаруживать и нейтрализовать вредоносные вирусы, а затем соответствующим образом уничтожать их самих. Из-за секретности со стороны военного департамента США, на сегодняшний день нет доступной и достоверной информации об инциденте. На этом этапе было совершено одно из первых киберпреступлений в США, в конце 70-х годов. Советник по компьютерной безопасности банка безопасности Pacific National Bank Стэнли Рифкин, который контролировал банковскую систему Лос-Анджелеса, раскрыл код, который через специальные компьютерные программы ввел на свой счет 10 миллионов долларов. Совершение данного преступления привлекло особое внимание ученых к информационной безопасности и противодействию киберпреступности.

Сделан вывод о том, что исследование первого этапа возникновения компьютерных вирусов как основного фактора совершения киберпреступлений в ряде западных стран такого вида киберпреступлений, как компьютерное мошенничество (в настоящее время мошенничество в сети Интернет) и компьютерное вымогательство (в условиях бурного развития ИКТ, вымогательство в виртуальном пространстве с угрозой раскрытия клеветнической информации), так называемая принудительная защита компьютерных систем, разработанная на территории бывшего СССР в 1979-1991 гг. В западных

странах США в конце 1970-х годов были зарегистрированы первые киберпреступления этого типа, основными жертвами которых стали финансово-кредитные организации. Одновременно на этом этапе были завершены первые исследования компьютерных вирусов, признанных основным средством совершения киберпреступлений, и разработаны первые антивирусные программы.

По мнению автора, второй этап в эволюции «компьютерных вирусов соответствует периоду середины 1980 по1992 год». В этот период были созданы компьютерные вирусы, адаптированные для работы на компьютерах с операционной системой MS-DOS. Распространение и повреждение этих вирусов происходило через компьютерные диски (дискеты).

Второй этап эволюции «компьютерных вирусов» не только привел к возникновению и причине совершения новых видов киберпреступлений, но и стал основой формирования преступлений, признавших Интернет средством совершения преступлений (злонамеренных программы и DoS-атаки), которые использовались для исполнения. Таким образом, сетевые ресурсы становятся объектом действий киберпреступников и представляют угрозу информационной безопасности.

Третий этап эволюции «компьютерных вирусов» в определённой степени связан с появлением глобальной информационно-коммуникационной сети Интернет, которая считается глобальной сетью нового поколения. В этот период появились вирусы, которые мешали не только нормальному функционированию компьютеров, но даже работе мобильных телефонов (например, 6 июня 2000 года был обнаружен первый компьютерный вирус Timofonica, повредивший мобильные телефоны).

Особенностью этого периода в эволюции «компьютерных вирусов» является проблема глобализации компьютерных устройств, которая каждый год бросает мировому сообществу выраженный вызов.

Анализ третьего этапа эволюции «компьютерных вирусов» показывает, что компьютерные вирусы разрабатываются непосредственно злоумышленниками для новых операционных систем, приложений для смартфонов и специализированного программного обеспечения, которые появляются на компьютерном рынке. Эволюция вирусов затрагивает сотни тысяч компьютеров по всему миру и уже нанесла ущерб в размере равном миллиардам американских долларов.

По мнению автора диссертации, четвертый этап эволюции «компьютерных вирусов» начался примерно в 2006-2007 годах и продолжается по сей день. В этот период количество «компьютерных вирусов» исчисляется сотнями миллионов. Все виды, в том числе и в виртуальном пространстве, уже получили широкое распространение. Если количество новых вредоносных программы компьютерных вирусов, обнаруженных «Лабораторией Касперского» за 15 лет (с 1992 по 2007), составляло около 2 миллионов, то к 2008, их число уже достигло 15 миллионов, в 2009 – 33 миллиона.

Во втором параграфе данной главы анализируется **«Понятие киберпреступлений».** Несмотря на многочисленные преимущества современных ИКТ, они создали новые условия, облегчающие совершение преступлений на национальном и международном уровне. Доходы от преступлений, связанных с ИКТ, являются третьими по величине в мире после доходов от торговли наркотиками и оружием. Это предоставляет благоприятную возможность для появления нового вида преступной деятельности, такого как киберпреступность, которая на современном этапе достигла очень высокого уровня. Примечательно, что правовое понятие «киберпреступность» «было впервые введено в 1978 году в законодательство США, которое означало «незаконный доступ к информации о личной жизни посредством специальных компьютерных программ». Определение, данное исследователями и экспертами ООН, представляет собой второе определение этого преступления после определения, данного законодательством США (1978 г.) и, конечно, не полностью отражает понятие киберпреступности, поскольку это опасное для общества деяние представляет собой не только незаконный доступ или незаконный сбор информации о личной жизни посредством специальных программ для ЭВМ или несанкционированное воздействие на автоматическую обработку и (или) передачу данных, но совершается с использованием различных средств ИКТ и их вспомогательного оборудования и причиняет различный материальный и моральный ущерб. Несмотря на большое количество преступлений с использованием ИКТ, в законодательстве Таджикистана нет закреплённого понятия «киберпреступность», что не дает возможности для правильной оценки и квалификации совершения данного деяния, определения причин и условий совершения данного преступления, предвидения его составных элементов и дополнения уголовного законодательства. В то же время, это очень важно не только для разработки правовых мер по противодействию этому виду преступлений на национальном уровне, но и для сбора сопоставимых статистических данных, развития единой системы учета на мировом уровне.

Диссертант утверждает, что в научной литературе термин «киберпреступность» в настоящее время используется наряду с термином «компьютерные преступления» и часто эти понятия используются как синонимы. Однако проведенные в этом направлении исследования, изучение уголовного законодательства постсоветских государств и зарубежных стран в этом направлении показывают, что данный термин не является синонимом «киберпреступности». Понятие «киберпреступность» является более широким и происходит как с использованием компьютеров, так и с использованием ИКТ и глобальной сети Интернет. На самом деле анализ терминологии показывает, что понятие киберпреступности шире по содержанию, сущности и средству совершения, опасности для общества, вине и противоправности, чем любое понятие, используемое в научной литературе как синоним этого термина. Если целью выявления преступлений является противодействие информационной безопасности совершения отдельных действий в отношении каждого

компьютера, даже если они не подключены к какой-либо сети, то киберпреступность обязательно подразумевает воздействие, которое осуществляется через ИКТ на удаленные устройства. Еще одно отличие выражается в том, что виды преступлений против информационной безопасности комплексно и подробно предусмотрены в отдельной главе уголовного законодательства, однако киберпреступлениями могут быть любые преступления, предусмотренные уголовным законодательством.

Для юридической науки в настоящее время необходимо разработать специальную систему понятий, которые обеспечат точное описание киберпреступности с точки зрения способа совершения и классификации этих действий. Поскольку данное общественно опасное деяние выступает серьезной проблемой для всего современного мирового сообщества с высоким уровнем латентности, наносит огромный материальный и моральный ущерб как национальной экономике, так и мировой безопасности и может быть совершено в киберпространстве с использованием ИКТ.

Автор отмечает, что для полного определения данного правового понятия в сфере информационных технологий уместно использовать слово «кибер». Термин «компьютерные преступления» по своему содержанию не может охватить все преступления в этой сфере. Понятие «киберпреступность» (англ. – cybercrime) значительно шире понятия «компьютерная преступность», поскольку позволяет более точно и полно определить характер преступления в ИКТ-пространстве.

Исследователь на основе анализа указанных мнений и исследования отраслевой литературы представляет понятие киберпреступности, представляющее собой совокупность преступлений в сфере информационных и телекоммуникационных сетей: «киберпреступность» – совокупность преступлений, совершаемых с использованием программно-технических средств и ИКТ в общем пространстве с целью незаконного получения, изменения информации, уничтожения или отмены информационных систем и ресурсов, направленных на причинение вреда конституционным правам и свободам человека и гражданина, государственной и общественной безопасности или имущественным отношениям.

В третьем параграфе диссертационного исследования анализируется «**Классификация киберпреступлений».**

В этом параграфе автор рассмотрел необходимость классификации киберпреступлений с учетом современной тенденции роста компьютеризации и большей зависимости населения от Интернета, а также постепенного и быстрого распространения киберпреступлений в различных формах. Поскольку предусмотренная уголовным законодательством квалификация общественно опасных деяний имеет особое юридическое значение, является обязательным признаком ужесточения норм уголовного законодательства, влияет на пресечение преступления, назначение наказания или определения способа совершения преступления, классификация киберпреступлений очень важна.

Некоторые ученые рассматривают классификацию киберпреступности по использованию ИКТ. Другие анализировали и рассматривали в зависимости от объекта посягательства, по системе работы компьютеров и интернет-сетей (по экспортным методам) и по характеру использования компьютерных сетей.

В этом параграфе автор классифицировал все киберпреступления по следующему признаку:

а) в зависимости от объекта преступного посягательства;

б) по характеру ущерба, причиненного компьютерной информации;

в) в зависимости от системы киберпреступлений;

г) в зависимости от способов совершения преступления;

Диссертант отмечает в зависимости от объекта преступного посягательства целесообразно классифицировать киберпреступления следующим образом:

а) посягательство на права и интересы владельцев компьютерной информации. Данная группа может совершать как опасные для общества действия, предусмотренные ст. 298 УК (незаконный доступ к компьютерной информации), так и предусмотренные ст. 303 УК РФ (разработка, использование и распространение вредоносных программ), а также «компьютерное мошенничество», «компьютерный саботаж», «компьютерный шпионаж»;

б) посягательство на права и интересы владельцев носителей информации. Опасные для общества действия, указанные в п. 3 м. 146 УК РТ, могут включать в себя (незаконное изготовление, передачу в чужое владение или владение в целях передачи в чужое владение специальных технических средств для негласного получения информации), ст. 304 УК РТ (нарушение правил использования компьютерной системы или сети), «несанкционированное использование защищенных программ для ЭВМ», «несанкционированное использование ЭВМ»).

Эти негативные последствия незаконных действий выражаются законодателем как альтернативные последствия и не отличаются друг от друга в зависимости от их относительной серьезности. Кроме того, законодатель различает причинение этого ущерба в зависимости от формы вины. Оно включает в себя, с одной стороны – умышленное уничтожение, ограничение, изменение или копирование компьютерной информации (ст. 298-304 УК РТ) и, с другой стороны – ответственность за причинение такого рода вреда по неосторожности (ч. 2 ст. 298, 299 УК РФ), 300, 303 и ч. 3 ст. 304 УК РТ).

В связи с этим, диссертант отмечает, что в зависимости от системы киберпреступления можно классифицировать следующим образом:

1. Преступления против сетей Интернет и поддерживающего их оборудования (деструктивные киберпреступления):

Преступления против сетей Интернет и поддерживающего их оборудования, повреждение данных и нарушение целостности данных и безопасности компьютерных систем. Такие преступления также могут привести к материальному ущербу.

2. Преступления, совершаемые с использованием сети интернет и электронных информационных ресурсов (социальных сетей мессенджеров и других ресурсов). Уголовный Кодекс Республики Таджикистан в 15 статьях (ст. 137, 137 (1), 144, 179 (1), 179 (3), 189, 241, 241 (1), 241 (2), 307, 307 (1), 307 (3), 373, 330, 334 (1) и 396), предусмотрены преступления, совершенные с использованием сети Интернет. К другим преступлениям, совершаемым с использованием сети интернет, можно отнести: ст. 109; ст. 247; ст. 200; ст. 250 УК РТ, но особых случаев использования сети интернет в диспозиции этих статей не указано.

3. Преступления, совершенные с использованием различных технических средств:

- Фишинговые письма;
- Кибер-сталкинг;
- Онлайн кража личных данных.

4. Преступления, ставящие в опасность жизнь и здоровье:

- Угрозы физического насилия;
- Кибersталкинг.

5. Преступление, связанное с нарушением тайны информации, например, незаконный доступ к компьютеру или компьютерной системе без нанесения ущерба информации.

Вторая глава диссертационного исследования – **«Уголовно-правовые вопросы борьбы с киберпреступностью на международном уровне»** состоит из трех параграфов**.**

В его первом параграфе – «**Международное сотрудничество в борьбе с киберпреступностью»** автор отмечает, что мировой опыт показывает, что киберпреступность трансформируется в транснациональные явления и оказывает негативное влияние на общество и безопасность всех государств, поэтому противодействие киберпреступности требует непосредственного международного сотрудничества с киберпреступностью. Сотрудничество государств, международных организаций, гражданского общества, частного сектора и экспертов выступает эффективным методом борьбы с киберпреступностью на международном уровне, поскольку возрастающее влияние информационных технологий, социальных сетей и Интернета на современную жизни человека, появилось множество полезных программ и средств связи, мессенджеров и других форм общения.

Автор подчеркивает, что в последние годы активно развивается правовая база и сотрудничество государств в направлении борьбы с киберпреступностью на международном, межправительственном и межведомственном уровне. В то же время в глобальном масштабе до сих пор не существует единого уголовно-правового механизма борьбы с киберпреступностью на международном уровне и не выработаны единые термины в этой сфере, что затрудняет сотрудничество государств в этой сфере.

Исследователь отмечает, что анализ Конвенции Европейского Союза о киберпреступности, предусматривающей международное сотрудничество в

борьбе с киберпреступностью, представляет собой прозрачный механизм международного сотрудничества государств и правоохранительных органов членов Конвенции по борьбе с киберпреступлениями и носит региональный характер. Однако, следует заметить, что региональный подход к унификации и координации уголовного законодательства внутри группы стран приводит к фрагментации международного сотрудничества в сфере борьбы с киберпреступностью, и не позволяет в полной мере обеспечить международное сотрудничество правоохранительных органов всех государств.

В диссертации показано, что сотрудничество государств в борьбе с киберпреступностью может основываться на международно-правовых документах (в рамках влиятельных международных организаций, в том числе ООН, СНГ, ОДКБ, ШОС) и межгосударственных правовых документах (контрактах, соглашениях и других двусторонних и многосторонних документах). Соглашения между государствами засекречены, поскольку такие формы сотрудничества в борьбе с киберпреступностью признаются современной и эффективной формой сотрудничества, секретность является важным аспектом реализации поставленных перед ними задач, а также наиболее благоприятной для достижения целей. Несмотря на то, что многие страны адаптировали свое уголовное законодательство к международному праву, в настоящее время не существует единого документа, который бы адекватно устранял проблемы уголовного права и устанавливал полноценное сотрудничество между государствами в этой сфере. В современном мире регулирование правоотношений при совершенствовании законодательства международного и национального уровня создаст благоприятные условия, и в этом контексте спорные вопросы в составе отдельных преступлений, в том числе киберпреступлений, мере необходимости найдут свое решение. Поэтому, в зависимости от транснационального характера и масштабов киберпреступности, наличия транснациональных цифровых доказательств автор разделил сотрудничество государств в направлении борьбы с киберпреступностью на следующие группы: национальное сотрудничество в борьбе с киберпреступностью; региональное сотрудничество; международное сотрудничество (межгосударственное, межправительственное и межведомственное сотрудничество).

Таким образом, международное сотрудничество в борьбе с киберпреступностью классифицируется в данном параграфе следующим образом:

– международное сотрудничество в области противодействия киберпреступности для создания универсальных, региональных и межгосударственных актов (Конвенция Европейского Союза по киберпреступности 2001 года (город Будапешт), Хартия Окинавы, «Соглашение о предоставлении цифровых инструментов и информационной безопасности», «Соглашение о сотрудничестве между странами-членами Содружества Независимых Государств в области противодействия компьютерным преступлениям», «Соглашение ШОС по обеспечению международной информационной безопасности», «Соглашение ШОС и СНГ о противодействии преступлениям в облас-

ти технологий», Программа сотрудничества стран – членов СНГ по противодействию преступлениям, совершаемым с использованием информационных технологий, на 2016-2020 годы и Соглашение между Правительством Республики Таджикистан и Правительством Туркменистана по обеспечению международной кибербезопасности и соглашение между Правительством Республики Таджикистан и Правительством Туркменистана о сотрудничестве в области технической защиты информации от 29 августа 2023 года, №381).

– международные организации по борьбе с киберпреступностью можно разделить на следующие типы:

1. Международные организации: а) Организация Объединенных Наций; б) Интерпол – международная организация уголовной полиции; в) Европол; г) Совет Европы;

2. Региональные организации: а) ШОС и б) ОДКБ.

Все эти организации играют важную роль в координации международных усилий, создании международного сотрудничества в борьбе с киберпреступностью.

Во втором разделе второй главы диссертационного исследования **«Ответственность за киберпреступность в соответствии с уголовным законодательством зарубежных стран и постсоветских государств»** диссертант указывает, что проблема противодействия киберпреступности, совершаемой посредством ИКТ, привлекла внимание государств мира. Для ее решения используются как меры политико-правового воздействия, так и средства технологического воздействия. Следует отметить, что вопросы обеспечения информационной безопасности, компьютерных технологий и их защиты от кибератак, в том числе посредством уголовного законодательства, по регулированию этого жизненно важного направления сегодня в большинстве развитых стран мира, являются актуальными. Уголовное законодательство разных стран базируется на политических, экономических, идеологических, религиозных, философских характеристиках, источниках и структуре правовых норм, а также других факторах, определяющих их характеристики. Сравнительный анализ уголовного законодательства зарубежных стран и стран постсоветского пространства помогает выявить общее и особое развитие норм, предусматривающих ответственность за совершение такого преступления.

С этой точки зрения уголовная ответственность в сфере киберпреступлений в системе уголовного права постсоветских стран имеет единую форму, отсутствие противодействия киберпреступлениям и круг противоправных действий в сфере киберпреступлений не включает. Постсоветские государства и иностранные государства можно условно разделить на две группы в зависимости от уголовной ответственности при совершении киберпреступлений:

– государства, в уголовном законодательстве которых предусмотрены особые нормы ответственности за совершение киберпреступлений;

– государства, находящиеся на стадии принятия соответствующих законов в связи с усилением уголовной ответственности в сфере киберпреступности.

На основе анализа ответственности за киберпреступления по уголовному законодательству зарубежных и постсоветских стран, принадлежащих к разным правовым семьям, автор сделал следующий вывод с точки зрения регулирования ответственности за киберпреступления.

В целях защиты безопасности информации от кибератак целесообразно тщательно изучить законодательство отдельных стран и на их основе регулировать внутреннее законодательство в этой области. XXI век нуждается в технологическом прогрессе. Тысячи операций осуществляются технологической компанией в тот момент, когда, если она не имеет правового регулирования, людям и в интересах государства, обществу наносится значительный имущественный ущерб. Мы должны принять практические меры на законодательном уровне, чтобы предвидеть масштабы киберпреступности и избежать этих нежелательных действий.

В отдельных государствах помимо уголовной ответственности действует ответственность административная. Это означает, что регулирование этих действий осуществляется не только через уголовное законодательство, но и через законодательство об административных правонарушениях (например, уголовное законодательство Австрии не считает нежелательные действия в секторе ИКТ преступлениями, однако административная ответственность за определенные нарушения предусмотрена в законе «О конфиденциальности данных», принятом в 2000 году).

Относительно большое количество наказаний содержится в Уголовном кодексе Азербайджана и Уголовном кодексе Франции: штрафы и лишение свободы. Напротив, в УК Бельгии предусмотрены два вида наказания (штраф и лишение свободы), УК Италии и Туркменистана (наказание в виде лишения свободы предусмотрено на срок до 3 лет), Узбекистана, Казахстана, Киргизии, Белоруссии и Украины (штраф, лишение свободы).

Уголовное законодательство зарубежных стран, составные элементы киберпреступности расположены в разных разделах.

Уголовный кодекс Республики Таджикистан признает уголовную ответственность только в отношении физического лица как субъекта этого преступления, однако в уголовно-правовых системах скандинавских и некоторых странах романо-германской правовой семьи субъектом может выступать и юридическое лицо. Однако некоторые страны, например, Италия, расширили сферу уголовной ответственности, указав другое лицо – должностное лицо.

В некоторых зарубежных странах ответственность за кражу, совершенную с использованием информационно-коммуникационных технологий, и мошенничество в сети Интернет предусмотрена специальная уголовная ответственностью – мошенничество (в России, Молдове) или за преступления мошеннического характера (в Великобритании, Австралии, США) находит свое выражение.

В третьем параграфе второй главы – **«Дифференциация уголовной ответственности за киберпреступления по уголовному законодательству зарубежных стран»** автор диссертации попытался проанализировать уголовное законодательство зарубежных стран, связанное с уголовной ответственностью за киберпреступления, и представить полезные научные выводы. Автор анализирует различные точки зрения и приходит к выводу, что разграничение уголовной ответственности является основным путем развития уголовного законодательства и уголовно-правовой политики Республики Таджикистан, решения теоретических и практических проблем уголовного права. Уголовно-правовая доктрина оценивается наличием ряда фундаментальных исследований, посвященных сущности, видам, способам и критериям разграничения уголовной ответственности. На основе анализа мнений ученых и изучения научной литературы в диссертации показано, что дифференциацию уголовной ответственности следует проводить по способу совершения преступления, предмету преступления, объективной стороне преступления и по отдельным статьям уголовного законодательства. Усилия законодателя по дифференциации уголовной ответственности, по мнению исследователя, направлены на достижение общей цели и в то же время правильны и адекватны по отношению к проблемам и угрозам современности, а также направлены на обеспечение уголовно-правовой защиты прав человека, общественных интересов и устранения больших рисков.

На основании этих высказываний, диссертант делает вывод о том, что во многих зарубежных странах рассмотрению данного вопроса было уделено большое доктринальное внимание. Анализ показывает, что новые виды киберпреступлений, в том числе: незаконное получение компьютерной информации, нарушение нормальной работы средств хранения, обработки или передачи информации, как правило, рассматриваются как преступления против личности, собственности или общественной безопасности.

В других странах принято различать уголовную ответственность за деликты, связанные с вмешательством в конфиденциальность, целостность и доступность самой компьютерной информации и средств ее хранения, обработки и передачи (средств автоматической обработки данных).

В отличие от законодательства других стран, ответственность за противоправные действия, связанные с разработкой, распространением и использованием заведомо вредоносных компьютерных программ или устройств, действиями, нарушающими без опасность данных или систем, распространением информации о сетевых идентификаторах, а также кибердействиями против преступности (средства аутентификации и пользователей) установлено следующее:

Основными отягчающими обстоятельствами признаками киберпреступности в уголовном праве других стран являются: 1) совершение преступления группой лиц; 2) совершение преступления в отношении объекта критической информационной инфраструктуры; 3) наступление тяжких последствий; 4) вредоносные компьютерные программы, компьютерная информа-

ция или средствах хранения, обработки или передачи незаконное использование; совершение преступлений с использованием различных технологических средств, специально предназначенных для воздействия.

Очень важно, что иностранные государства предоставляют возможность привлекать юридических лиц к уголовной ответственности за многие киберпреступления.

При этом важной особенностью зарубежного законодательства является наличие норм, обосновывающих применение традиционных уголовно-правовых норм к новым «цифровым формам преступности».

Таким образом, эти страны без изменения существующих правовых структур, по-видимому, на законных основаниях расширяют сферу своих действий и тем самым рассматривают вопрос о пересмотре признаков состава этих традиционных преступлений.

Для решения существующих проблем в направлении киберпреступности, которая является новым явлением в наше время, необходимо использовать правовой опыт развитых стран и учитывать обстоятельства, применимые к практике данного вида преступлений, при разработке законодательства. Для борьбы с данным видом преступлений считается эффективным регулирование правоотношений в цивилизованных обществах.

Таким образом, в связи с дифференциацией ответственности за киберпреступления по уголовному законодательству зарубежных стран в зависимости от способа совершения киберпреступлений государства можно разделить на 2 группы.

К первой группе относятся такие правонарушения, как невыполнение провайдерами решений киберпреступников о блокировке соответствующих Интернет-ресурсов и удалении запрещенной информации, виртуальная (виртуальная) помощь совершении киберпреступлений и использование Интернет-ресурсов в целях распространения информации. Уголовная ответственность предусмотрена в зависимости от способа совершения преступления (например, статьи 285A, 286A, 287A и 287B Уголовного кодекса Китая). Однако в некоторых странах деяния, предусмотренные статьей 285A УК КНР, влекут за собой административную, а не уголовную ответственность (например, статья 13.34 Кодекса Российской Федерации об административных правонарушениях).

Вторая группа включает страны, криминализирующие преступления, связанные с использованием ИКТ, в том числе интернет-мошенничество. В качестве примера можно привести Уголовный кодекс Республики Молдова (статья 260 (5)), Уголовный кодекс Российской Федерации (статья 159 (6)), Закон о мошенничестве Великобритании 2006 года, Уголовный кодекс Испании (статья 248), Уголовный кодекс Бельгии (статья 147), Уголовный кодекс Дании (статья 279 (a)) и Уголовный кодекс Эстонии (статья 213).

Третья глава – **«Уголовно-правовая характеристика преступлений против сетей Интернет и их вспомогательного оборудования»** состоит из трех параграфов.

Первый параграф третьей главы – «**Объект преступлений против сетей Интернет и их вспомогательного оборудования (вредоносные программы, DoS-атаки)»** посвящен анализу объекта преступления с точки зрения науки уголовного права.

В работе отмечается, что вопросы изучения объекта преступления являются такими же важными, как и вопросы изучения вины в уголовном праве, однако в юридической литературе данная проблема на сегодняшний день остаётся малоизученной. Однако, поскольку компьютеры и информационно-коммуникационные технологии используются для многих общественно опасных деяний, предмет преступления оценивается иначе, чем в «традиционной» терминологии интернет-сети и сопутствующем им оборудовании. Поскольку современный мир невозможно представить без технического прогресса, все пользователи современных информационно-коммуникационных технологий в своей деятельности сталкиваются с негативными последствиями вредоносных компьютерных программ, и DoS-атаками. Эти виды антивирусных программ нельзя разделить на несколько категорий. Некоторые из них относительно безвредны, другие же способны нанести непоправимый ущерб не только информационным активам, но и самому компьютерному оборудованию. Автор отмечает, что проблемы объекта преступлений против сетей Интернет и их вспомогательного оборудования, включая вредоносные программы и DoS-атаки, в настоящее время весьма спорны и связаны с данным вопросом лишь 2% от общего количества выполненных исследований направлены на эту проблему, что в условиях бурного развития информационных и коммуникационных технологий является весьма тревожной оценкой. На основе всестороннего анализа научной литературы диссертант утверждает, что общий объект этих преступлений охватывает общественные отношения и общественную безопасность. В связи с этим общественные отношения, которые наносят вред вредоносным программы и DoS-атакам, особенно важны для общества, их защита должна осуществляться наиболее эффективными и действенными мерами.

Другой вопрос, который диссертант проанализировал в данном параграфе, – это видовой объект преступлений против сетей Интернет и их вспомогательного оборудования. Исследователь утверждает, что на современном этапе развития науки уголовного права можно увидеть и другие точки зрения по вопросу о видовом объекте преступления. Мнения исследователей не совпадают в вопросах определения видового объекта преступлений против сетей Интернет и их вспомогательного оборудования. Преступления против сетей Интернет и их вспомогательного оборудования (вредоносные программы, DoS), по сути, закреплены в главе 28 УК РТ «Преступления против информационной безопасности».

В связи с этим в работе делается вывод, что объектом преступлений против сети Интернет и её вспомогательных устройств являются права и интересы личности, реальные, юридические, общественные и государственные в отношении компьютерной информации, информационных ресурсов, охра-

няемых уголовным законом важных общественных отношений в сфере безопасности разработки, использования распространения информационных ИКТ-системе использования автоматизированных систем обработки данных.

Автор отмечает, что одним из критериев признания преступлений против интернет-сетей вспомогательного оборудования (вредоносные программы, DoS-атаки) в главе 28 УК РТ является непосредственный объект преступления – совокупность общественных отношений в сфере правомерного и безопасного использования компьютерной информации, к которой относятся информационные ресурсы. Непосредственным объектом преступлений против сетей Интернет и их вспомогательного оборудования являются следующие общественные отношения, которые мы классифицируем следующим образом: 1) обеспечение законного доступа, создания, обработки, преобразования и использования компьютерной информации; 2) добросовестная деятельность МЭХ или их сети; 3) деловые интересы, связанные с продажей данного компьютерного оборудования. В качестве непосредственного объекта данного преступления, повлекшего по неосторожности тяжкие последствия, предусмотренные частью 2 статьи 303 УК РТ выступают общественные отношения, которые в зависимости от их характера затрагивают иные общественно значимые ценности (жизнь человека, здоровье человека и т. д.).

Дополнительным объектом этих преступлений являются общественные отношения, которые регулируются правовыми нормами и обеспечивают права и законные интересы человека, общества и государства.

На основе рассмотрения и анализа объекта преступлений против сетей Интернет и их вспомогательного оборудования диссертантом сделан вывод о том, что эти общественно вредные действия (вредоносные программы, DoS-атаки) наносят вред не только информационной безопасности, но и различным связям с общественностью или большой неопределённой группе людей (например, в случае кибертерроризма) причиняет вред или несёт угрозу причинения такого вреда. Отечественным уголовным законодательством предусмотрена категория этого преступления в главе 28 «Преступления против информационной безопасности», а с учетом иных общественных отношений, включенных в данную главу (кибертерроризм, киберэкстремизм, кибersталкинг, фишинговые письма). Считаем целесообразным введение в УК РТ нового дополнительного раздела под названием «Преступления против кибербезопасности».

Автор указывает, что использование дополнительного объекта не является обязательным. Его существование направлено на защиту прав и законных интересов личности, общества и государства. Дополнительными объектами являются, например, собственность, авторское право, неприкосновенные права, личная и семейная тайна, экологическая безопасность, основы конституционного строя Республики Таджикистан. Наличие дополнительных объектов, несомненно, повышает общественную опасность преступления должно учитываться при назначении справедливого наказания виновному. Дополнительным объектом данных преступлений являются обществен-

ные отношения, которые регулируются правовыми нормами и гарантируют права и законные интересы личности, общества и государства.

Во втором параграфе третьей главы – **«Объектная сторона преступлений против сетей Интернет и их вспомогательного оборудования (вредоносных программ, DoS-атак)»** изучаются признаки объективной стороны преступлений против сетей Интернет и их вспомогательного оборудования.

Автор отмечает, что для выявления данных деяний и последующего привлечения к ответственности лица, их совершившего, важно установить признаки объективной стороны данных преступлений. В диссертации отмечается, что признаки объективной стороны конкретного преступления находят отражение в диспозиции статей особенной части Уголовного кодекса Республики Таджикистан. Если в диспозиции норм нет индикатора наличия опасных для общества последствий, то этот состав преступления является формальным. Таким образом, преступление считается оконченным с момента совершения общественно опасного деяния. Следовательно, объективная сторона преступления имеет специфические признаки, разделяющие их на две группы: во-первых, обязательные признаки – общественно опасное деяние (действие или бездействие, последствия деяния и причинно-следственная связь), во-вторых – дополнительные признаки. Объективную сторону преступлений против сетей Интернет и их вспомогательного оборудования представляют общественные отношения, которые в результате их совершения наносят вред информации, содержащейся в компьютере или компьютерной системе, сети Интернет и их вспомогательном оборудовании (модем, Wi-Fi, роутер, специальные антенны, спутниковое, мобильное оборудование) (в том числе средства совершения преступлений, такие как сетевые черви, классические файловые вирусы, трояны, хакерские инструменты и другие программы). В результате проведённого исследования в области преступлений против сетей Интернет и их вспомогательного оборудования (вредоносные программы, DoS-атаки), считает, что объективная сторона выражена в следующих действиях: разработка вредоносных компьютерных программ, уничтожающих, блокирующих, изменяющих или копирующих информацию, сохранение данных в компьютерных режимах, сетях либо компьютерных базах информации без разрешения; введение изменений в имеющиеся программы вместе с мишенью ликвидирования, блокировки, перемены либо коприрования данных, хранящихся в компьютерной концепции либо узы, либо в основе информации машины, без позволения; создание специализированных вирусных проектов (равно как типы вредных проектов); популяризация загон информации, включающих специализированные проекта, которые содержат вирусы; заключение с эксплуатации компьютерного оснащения; несоблюдение компьютерных сеток; атаки, направленные на нарушение работы сетей связи и маршрутизаторов (суть этой атаки заключается в отправке на атакуемый компьютер большого потока так называемых флудов, то есть неверных или по сути бессмысленных запросов. Этот фактор полностью блокирует все сети передачи данных или входящий мар-

шрутизатор. Поскольку объем данных превышает объем ресурсов обработки, получение правильных пакетов данных от других пользователей становится невозможным. В результате система перестает обслуживаться, атаки, направленные на пополнение операционной системы или программных ресурсов (эти типы атак направлены не на коммуникационную сеть, а на саму систему. Каждая система имеет множество ограничений по различным пропускным способностям (время процессора, дисковое пространство, память и т.д.). Целью такого взаимодействия является перенаправление системы на преодоления этих препятствий. Для этого на компьютер пострадавшего отправляется большое количество запросов. В результате этого действия сервер, система выдаёт сбой обслуживания запросов законных пользователей).

Автор указывает, что способ, орудие, средство, место, время и условия (обстановка) совершения преступления выступают факультативными признаками объективной стороны. В случаях, когда эти признаки предусмотрены нормами уголовного права, они выступают обязательными признаком конкретного преступления.

Средства совершения преступлений – это объекты, которые используются для облегчения совершения преступлений, например, инструменты для совершения преступлений против сетей Интернет и поддерживающего их оборудования, сетевые черви, классические файловые вирусы (один из видов вредоносных программ), трояны, хакерские инструменты, шпионские программы и организует программы вымогательства и шифрования.

В третьем параграфе третьей главы – **«Субъективные признаки преступлений против сетей Интернет и их вспомогательного оборудования (вредоносные программы, DoS-атаки)».** Автор отмечает, что преступление как общественно опасное деяние совершается при наличии вместе всех составляющих признаков преступления – объективных и субъективных. Общность этих признаков выражается в том, что они по-разному оценивают сущность преступления. Для правильного применения норм уголовного законодательства важен детальный анализ всех признаков состава преступления. Исследователь указывает, что по вопросу преступлений против сетей Интернет и их вспомогательного оборудования (вредоносных программ, DoS-атак) в науке уголовного права существует множество мнений, при этом не существует единой и конкретной позиции. Некоторые ученые считают, что необходимо установить возраст уголовной ответственности за совершение преступлений против сетей Интернет и их вспомогательного оборудования (вредоносных программ, DoS-атак) с 14 лет, другие исследователи категорически выступают против этой меры.

Согласно суждению диссертанта, субъектом преступления против сети интернет и вспомогательного оборудования является вменяемое физическое лицо, достигшее четырнадцати летнего возраста, потому как именно в данном возрасте индивид осознает значимость компьютерных данных, компьютерных сетей, а также понимает принципы и методы их использования. Важнее всего то, что в условиях глобализации ИКТ доступны для лиц, не дос-

тигших четырнадцатилетнего возраста, осведомлённых об опасности нарушения правил использования кибернетических технологий, в этом части компьютерной данных.

Рассматривая вопрос о субъекте данного преступления, автор приходит к выводу о том, что в качестве субъекта преступления против сетей Интернет и их вспомогательного оборудования (вредоносные программы, DoS-атаки), может выступать любое физическое лицо (т. е. общий субъект преступления), достигшее 14-летнего возраста во время совершения преступления. В связи с этим, диссертант считает необходимым включить в часть 2 статьи 23 УК РТ (о возрасте наступления уголовной ответственности) состав преступлений, предусмотренных статьями 300 и 303 УК РТ и дополнить нормой об уголовной ответственности за такие преступления для лиц с 14 лет.

По мнению автора, снижение возраста уголовной ответственности для физического лица до 14-летнего возраста, вполне приемлемо, но этот процесс возможен лишь в тех случаях, когда имеются серьезные последствия для сетей Интернет и вспомогательного оборудования (вредоносные программы, DoS-атаки), или риск, вызвавший их вспышку. (например, за совершение квалифицируемых преступлений, предусмотренных статьями 300 и 303 УК РТ) допустимо. Для обоснования данной точки зрения можно сослаться на опыт ряда зарубежных стран (уголовное законодательство Франции, Швеции, Латвии, Дании), в которых уголовная ответственность за совершение преступлений против сетей Интернет и поддерживающего их оборудования (вредоносных программ, DoS атаки) нацелена на возрастные категории 14 или 15 лет. При этом снижение возраста уголовной ответственности за указанные выше преступления обосновывается следующим: 1) социальная сущность таких деяний хорошо осознаётся лицами в возрасте 14 или 15 лет; 2) такие деяния имеют высокий характер общественной опасности; 3) эти преступления широко распространены среди лиц в возрасте 14 или 15 лет.

Автор указывает, что глобализация, бурное развитие коммуникационных информационных технологий и их вредные последствия в настоящее время признаются большинством развитых стран мира, а в их уголовном законодательстве в качестве субъектов преступлений против сетей Интернет и их вспомогательного оборудования (вредоносных программ, DoS-атаки) признаются также юридические лица.

Автор диссертации отмечает, что наличие признаков преднамеренных действий, согласно исследованиям, проведенным по развитию вредоносных программ и DoS-атакам, требует комплексной проверки. С этой точки зрения наличие вредоносности программы является подтверждением прямого намерения совершить преступление. Субъективная сторона преступлений против сетей Интернет и их вспомогательного оборудования характеризуется лишь прямым умыслом киберпреступника в связи с тем, что последний осознаёт опасность совершаемых им действий, предвидит возможность или неизбежность их опасных последствий для общества, тем не менее желает их наступления.

Четвертая глава – **«Уголовно-правовая характеристика преступлений, совершенных с использованием различных технических средств»,** состоит из трех параграфов. Первый параграф посвящен **«Объекту преступлений, совершенных с использованием различных технических средств (фишинговые письма, кибersталкинг, кража онлайн-личности)».**

По мнению автора, для квалификации любого преступления необходим уголовно-правовой анализ состава преступления. Состав преступления является одним из центральных институтов уголовного права. Основанием уголовной ответственности, особенно за киберпреступления, является деяние, содержащее все признаки преступления (ст. 11 УК РТ). Одним из признаков состава преступления, имеющих значение для задержания, является объект преступления. Объект преступления при анализе любой нормы особенной части УК ставится на первое место как элемент состава преступления, особенно киберпреступлений, поскольку правильное определение объекта преступления позволяет понять социальную сущность этого преступления, определить его место среди других общественных отношений, а также определить степень опасности для общественных интересов, охраняемых законом. В связи с этим, в результате исследования юридической литературы, автор приходит к выводу о том, что в качестве объекта преступлений с использованием разных технических средств могут быть общественные отношения (к примеру, в области обеспеченья защищенности компьютерных данных) и разные личные интересы (жизнь, здоровье, личная переписка и другие материальные и нематериальные блага), а также единичных права и интересы физических и юридических лиц, правоотношения которые охраняются законодательством.

В связи с тем, что глава 28 УК РТ предусмотрены «Преступления против информационной безопасности», автор предполагает, что информационная безопасность является родовым объектом данных преступлений.

Видовым объектом преступления, которое совершается с помощью применения разных технических средств, представляются общественные отношения, которые обеспечивают безопасность лица, общества и государства от внутренних и внешних киберугроз в виде сохранения, передачи а также использования информации, которая обеспечивает охрану конституциональных прав и свобод, а также национальной независимости, территориальной целостности и экономическое и социальное развитие Таджикистана, а также безопасность государства.

В качестве непосредственного объекта данного деяния выступают: достоинство, репутация, право на неприкосновенность личной жизни, частные и семейные тайны, право человека на переписку, авторские и смежные права гражданина, имущественные отношения, общественные отношения, обеспечивающие защиту коммерческой, налоговой, банковской информации от неправомерного доступа к ней. Автор обосновывает это мнение тем, что преступления, совершаемые с использованием различных тех-

нических средств (фишинговые письма, кибersталкинг, кража онлайн-личности), по сути выражаются в том, что киберпреступники используют Интернет для ежедневного распространения ложной рекламы в социальных сетях, обманным путем завоевывая доверие граждан и получения прав на имущество, личную информацию, путем отправки сообщения о том, что гражданин выиграл в лотерею, или получил право на финансовую поддержку, участие в инвестиционных проектах мошеннических иностранных компаний, получил предложение финансовой помощи от политиков и щедрых людей, завещания денег от какого-либо дальнего родственника, подарки из-за границы в виде «посылок» и тому подобное, распределяющий, организующий и управляющий путем обмана с целью хищения денежных средств граждан.

Второй параграф четвертой главы посвящен **«Объективной стороне преступлений, совершаемых с использованием различных технических средств (фишинговая письма, кибersталкинг, кража онлайн-личности)».**

Исследователь отмечает, что наряду с другими признаками состава преступления, объективная сторона преступления занимает важное место в определении состава этого преступления. Известно, что объективной стороной преступления является возникновение опасного для общества деяния, причиняющего вред объекту, охраняемому уголовным законом. Она состоит из совокупности признаков, описывающих внешнюю сторону опасного для общества деяния. Этот состав преступления имеет основные и факультативные признаки.

В результате анализа мнений ученых, в диссертации делается вывод, что объективная сторона преступлений, совершаемых с использованием различных технических средств, включает в себя совокупность признаков, которые указывают на внешние установки человека, связанные с незаконным сбором информации о другом лице, распространение информации в широком диапазоне, до публичного показа путём распространения в средствах массовой информации, а также рассылка мошеннических электронных писем при использовании сети Интернет, наносящая ущерб правам и законным интересам потерпевшего.

Одним из факультативных признаков выступает место совершения преступления. В связи с тем, что эти преступления совершаются через интернет-сети, место совершения этих преступлений совершенно не имеет значения для их квалификации преступления. Уголовное законодательство также не предоставляет преимуществ в данном вопросе. В связи с этим, рассмотрение места совершения этих преступлений не имеет абсолютно никакого значения.

Еще одним из факультативных компонентов является способ совершения преступления. Способ совершения преступления – это совокупность методов и способов, которые виновный использует при совершении общественно опасного деяния.

Из содержания норм УК РТ следует, что способ совершения преступления описан в объективной сторона преступления. Например, УК РТ в разделе о преступлениях против информационной безопасности обычно устанавливаются такие нормы, как «мошенничество», «использование сети Интернет», «незаконный доступ к компьютерной информации» и т.д., которые признается как виды совершения преступления. В связи с этим, исследователь обратился к теории науки об ужесточении уголовного законодательства. Автор отмечает, что способ совершения таких преступлений как фишинговые письма, кибersталкинг, кража онлайн-личности целесообразно рассматривать отдельно, так как способ совершения этих преступлений осуществляется двумя способами: 1) отправка писем путем обмана; 2) их совершение через интернет.

Третий параграф четвертой главы направлен на анализ **«Субъективных признаков преступлений, совершаемых с использованием различных технических средств (фишинговые письма, кибersталкинг, кража онлайн-личности)».**

Диссертант отмечает, что уголовное законодательство не предусматривает ответственности за киберпреступность, совершаемую с использованием различных технических средств (фишинговые письма, кибersталкинг, кража онлайн-личности), но развитие совершения этих преступлений в мировом обществе развивается день ото дня. Выявление субъективных признаков этих преступлений имеет важное теоретическое и практическое значение при использовании различных технических средств для совершения преступления. Субъективные признаки указанных преступлений, как и субъективные признаки других преступлений, в целом включают два составляющих элемента 1) субъективная сторона; 2) субъект преступления.

Автор отмечает, что субъективная сторона рассматриваемых преступлений имеет различные формы совершения, характеризующие внутреннюю (психическую) сторону киберпреступника. Субъективная сторона заключается в том, что эти преступления совершаются в форме непосредственного умысла и выражаются в намерении приобрести имущество, незаконно получить личную информацию, преследовании лица, блокировке информации и ее уничтожении, что характеризуется в качестве «корыстной» цели. Корыстной целью совершения этих преступлений является умышленное причинение другому лицу имущественного или неимущественного ущерба, нанесенного личной жизни лица и использованию этих данных против него, а также иных действий (совершение налогового мошенничества или медицинского страхования от имени потерпевшего и т.д.).

По мнению автора, субъективные признаки преступлений, совершаемых с использованием различных технических средств (фишинговые письма, кибersталкинг, кража онлайн-личности), заключаются в основном в получении информации, содержащейся в компьютерных системах, компьютерных сетях и машинных базах данных, незаконном завладении ею, общественной опасности этого действия. Характеризуется исключительно прямым

умыслом, проявляющемся в желании совершить деяние. В квалифицирующих составах, субъект осознает способы совершения преступления (применение насилия или угроз с его использованием, запугивание, высмеивание, привлечение внимания, получение информации, нарушение безопасности, манипулирование другими людьми с помощью угроз) и желает совершить это опасное для общества деяние именно этими способами.

Субъекты этих преступлений могут быть как общими, так и специальными. Эти типы преступлений могут быть совершены людьми, которые хорошо разбираются в ИКТ и программировании и знакомы с общей деятельностью интернет-сети. Именно этот фактор дает им возможность совершить этот вид преступлений. При совершении этих преступлений не имеет значения, является ли человек сотрудником той или иной организации или учреждения. Обычные граждане также могут совершать эти преступления.

Наряду с указанными субъектами данного преступления могут быть признаны также операторы и провайдеры, если они распространяют или рекламируют посредством служб электронной связи любую информацию, направленную против основ конституционного строя, личной, общественной, государственной безопасности, информацию об ограничении прав и свобод человека и гражданина, разжигающую религиозную, межнациональную, межрасовую, или региональную рознь. А также если их действия направлены на нанесение ущерба национальной чести и репутации, рекламу способов изготовления и продвижения наркотических средств, взрывчатых и других отравляющих веществ, на совершение преступлений и административных правонарушений, имеющих экстремистский и террористический характер, распространение порнографии, в том числе детской или распространение любой другой информации, запрещенной судебными актами, вступившими в законную силу и законодательством Республики Таджикистан.

Пятая глава диссертационного исследования – **«Криминологическое исследование киберпреступности»** состоит из трех параграфов.

В его первом параграфе – **«Состояние, структура и динамика киберпреступности»** есть существенные особенности, связанные с цепочкой анализа. Автор придерживается мнения, что в современном обществе киберпреступность стала организованным и массовым явлением, от которого во многом зависит регулирование общественных отношений, потому что эти сложные факторы связаны с поиском необходимой информации, касающейся состояния, структуры и динамики киберпреступлений.

В диссертации указывается, что большая часть преступлений, совершаемых в сфере киберпреступлений, приходится на сферу водных, энергетических и мобильных компаний, а ущерб, причиненный в этих сферах, исчисляется миллионами сомони. Сотрудниками Министерства внутренних дел Республики Таджикистан в период с 2018 по 2020 годы раскрыто только 43 из 51 совершенного киберпреступления, то есть 84%. Ситуация, когда такие преступления не раскрываются, считается тревожной и представляет собой реальную угрозу национальной безопасности и информатизации. Данный

процесс проводят даже государства-члены СНГ, так как в 2020 году в СНГ доля уголовных дел, поданных по обвинительному приговору, переданных в суд составила 18,2% (2018 – 24,8%, 2019 – 23%) из общего числа зарегистрированных преступлений в этом направлении. Следует заметить, что 73,6% из них не были раскрыты в 2020 году (2018 – 66,5%, 2019 – 68,4%). Посредством изучения данных, автор приходит к выводу о том, что чрезмерное совершение киберпреступлений наблюдается в Российской Федерации, Республике Беларусь и Азербайджанской Республике. Так, статистика киберпреступлений в государствах-участниках СНГ показывает, что в 2020 году количество зарегистрированных преступлений в сфере киберпреступлений выросло в 4 раза, то есть с 125 244 случаев в 2018 году до 536 516 случаев в 2020 году.

Свои выводы в диссертации по криминологическому исследованию киберпреступлений автор излагает в следующем виде:

– В настоящее время наблюдается рост совершения киберпреступлений с использованием ИКТ. В связи с этим необходимо пересмотреть образовательные программы и государственные стандарты, принятые в этом направлении, увеличить количество и улучшить качество подготовки специалистов в области кибербезопасности, а также повысить квалификацию существующих сотрудников, работающих в этом направлении. Аргументируется необходимость за счет привлечения ученых отрасли, квалифицированных технических специалистов, ветеранов отрасли, создать учебный институт в области обеспечения информационной безопасности от кибератак, что принесёт пользу, поскольку исследования показали, что одним из основных элементов обеспечения информационной безопасности от кибератак и предотвращения киберпреступлений – это развитие образовательного и научного потенциала страны.

– Официальная статистика Главного информационно-аналитического центра Министерства внутренних дел Республики Таджикистан не полностью отражает фактический объем и характер кибератак.

– Киберпреступники обладают обширными знаниями в области использования Интернета, различных технических средств и разработки вредоносных программ. Поэтому борьба с киберпреступностью должна осуществляться с привлечением специалистов, изучивших эти особенности.

– Самая большая угроза безопасности защищенной компьютерной информации исходит от внутренних пользователей системы. В связи с этим особое значение приобретает повышение профессионального уровня специалистов и контроль за их надежностью со стороны службы безопасности компании.

– Неосведомлённость жертв киберпреступности об основных инструментах и методах защиты своей информации позволяет злоумышленнику легко совершать противоправные действия. В связи с этим, в средствах массовой информации важно отразить наиболее распространенные планы киберпреступлений и способы их предотвращения, а также развивать у населе-

ния навыки обработки компьютерной информации и обучение работе с различными техническими устройствами, в том числе с сетью Интернет.

– Большинство из жертв киберпреступности являются юридическими лицами. В связи с этим, предприятиям и организациям необходимо уделять пристальное внимание обеспечению компьютерной безопасности от кибератак, в бизнес-плане определить должность специалиста по защите информации и принять меры для ее реализации.

– Высокая степень киберпреступности больше связана с трудностью выявления киберпреступников и нежеланием жертвы сообщать об этом в правоохранительные органы.

– Одной из основных тенденций развития киберпреступности является ее несвоевременное обнаружение. Этому процессу способствует незаконное создание информационно-коммуникационных сетей, мессенджеров и Интернета. Использование новых технологий в финансовых и кредитных операциях, онлайн-бизнесе, шифровании данных и т.д., не позволяет государству и обществу вовремя предотвратить большое количество киберпреступлений, поскольку они игнорируются по технологическим причинам.

Во втором параграфе пятой главы исследован вопрос – **«Криминологическая характеристика личности киберпреступника».** В диссертации показано, что успешное предупреждение преступлений возможно только при условии, если особое внимание уделено личности преступника. Поэтому необходимо отметить, что такая категория, как личность преступника, является основным и важным элементом всех механизмов преступного поведения. Специфические характеристики, вызывающие преступное поведение, должны быть непосредственным объектом профилактических и предупредительных мер. Поэтому вопрос о личности преступника входит в число приоритетных и в то же время является одним из актуальных вопросов. Вопрос о личности преступника представляется одним из важных вопросов науки криминологии, он является неотъемлемой частью предмета этой науки. Эта концепция особенно важна для киберпреступности, поскольку она является чрезвычайно важным элементом обнаружения и расследования преступлений.

По мнению автора важным является классификация преступления на категории в зависимости от действий преступника, осуществляемых посредством ИКТ. Таких способностей четыре уровня, каждая из этих групп имеет свои особенности.

Первый уровень – минимальная возможность ведения диалога в автоматической системе, реализуется путем запуска специальных программ обработки информации;

Второй уровень включает в себя способность разрабатывать и запускать отдельные программы обработки информации в современной технологической форме;

Третий уровень дает возможность контролировать работу системы и напрямую влиять на ее основные программы;

Четвертый уровень охватывает все возможности людей, проектирующих, внедряющих и ремонтирующих техническое оборудование данной технологической системы. Опыт показывает, что киберпреступник является высококвалифицированным специалистом и знает все тонкости технологической и информационной системы.

Автор, опираясь на достоверные источники о различных аспектах личности киберпреступников (уголовное дело, официальный статистический отчет, результаты криминологических исследований), разделил таких лиц на следующие группы:

1. В зависимости от типа киберпреступности и уровня навыков работы с компьютерными системами:

– лица, имеющие высшее образование в данной области, имеющие опыт совершения киберпреступлений и считающиеся обладателями специальных знаний. Наличие специальных знаний означает принадлежность такого преступника к группе хакеров (взломщиков);

– лица, ранее совершившие преступления и прошедшие «специальную подготовку» в качестве киберпреступников, которых заинтересовали широкие возможности киберпространства, а также представители организованной преступности, способные объединить людей, обладающих специальными знаниями, для совершения преступлений и предпринять усилия, направленные на получение прибыли.

2. Состояние профилактики преступной деятельности:

– свою основную преступную деятельность они осуществляют только в киберпространстве. В то же время, если его вовремя предотвратить, опасное поведение таких лиц существенно контролируется;

– совершение преступных действий в виртуальном пространстве и в реальной жизни.

3. В зависимости от причин преступного деяния:

– жадный вид формируется лицами, которые имеют явную склонность к преследованию материальных интересов и других важных факторов (спортивных наград и т.д.) через совершение киберпреступности;

– насильственный вид. Отсутствие физического контакта в виртуальном пространстве не исключает совершения преступлений против личности (угрозы самоубийства, угрозы убийством) способами психологического воздействия, киберпреследования, запугивания, а также подстрекательства к насильственным нападениям;

– вид социальной дезорганизации или термин, называемый «игра». Основная цель киберпреступника – нарушить социальные и правовые нормы, оказать деструктивное воздействие на общество и общественные отношения;

– вид протеста. Киберпреступность как форма протеста, способ политической или идеологической борьбы;

– саморегулирующийся тип. У преступников есть желание получить более высокий неформальный социальный статус в киберпространстве;

4. В зависимости от психологических особенностей характера киберпреступника их можно разделить на следующие группы:

– тип желания;

– тип социального неблагополучия;

– тип с идеологическими и политическими характеристиками;

– тип киберпреступника варьируется зависимости от ситуации.

В третьем параграфе пятой главы рассматривается вопрос **«Анализ, предупреждения и профилактики киберпреступлений».**

Автором отмечается, что одной из важнейших задач правоохранительных органов, живущих в современную эпоху формирования новых рыночных отношений, является регулирование развития демократического общества, связанного с бурным развитием информационных технологий. В связи с этим, первостепенное значение приобретает борьба с киберпреступностью, и особенно с разработкой, использованием и распространением вредоносных программ, DoS-атак, кибersталкинга, фишинговых писем, кражи онлайн-личности. Автор выразил актуальность изучения проблемы киберпреступности в двух аспектах: во-первых – стремительное расширение масштабов разработки, внедрение и использование новых информационных технологий; во-вторых – стремительное использование новых технологий для достижения противоправных целей и преобладание инновационных технологий, в том числе информационных, в криминальной среде.

В современных условиях сфера киберпреступности, а также информационно-коммуникационных технологий стремительно развивается. Угрозы информационным ресурсам постоянно растут и развиваются. Таким образом, основное направление деятельности по борьбе с киберпреступностью базируется на принятии следующих организационных и технических мер:

1. Обеспечение необходимого уровня безопасности государственных информационных систем и ресурсов, их целостности и конфиденциальности, реализация единых требований по защите информации от несанкционированного доступа или изменения данных, воздействия компьютерных атак и вирусов, а также использование сертифицированных отечественных средств предотвращения и обнаружения компьютерных атак и защищенной информации, предоставляемых организациями, получившими необходимую лицензию в установленном порядке;

2. Использование криптографических средств защиты информации является обязательным для информационных систем и ресурсов, содержащих сведения, составляющие государственную тайну;

3. Контроль за использованием и защита государственных информационных систем и ресурсов от противоправных действий должны обеспечиваться на основе создания системы контроля и учета операций при работе с государственными информационными системами и ресурсами;

4. Обеспечение комплексного подхода к решению вопросов информационной безопасности от кибератак, с учетом необходимости дифференциации ее уровня в различных государственных органах;

5. Разработка модели угроз информационной безопасности от кибератак;

6. Определение технических требований и критериев идентификации важных объектов инфраструктуры информационных технологий, создание реестра важных объектов, разработка мер их защиты и средств контроля соблюдения соответствующих требований;

7. Обеспечение эффективного мониторинга состояния информационной безопасности;

8. Совершенствование нормативной, правовой и методологической базы в области защиты государственных информационных систем и ресурсов;

9. Организация единого порядка согласования технических условий обеспечения информационной безопасности государственных информационных систем и ресурсов;

10. Сертификация государственных информационных систем и ресурсов в деятельности государственных органов, используемых уполномоченными государственными органами, и контроль их соответствия требованиям информационной безопасности;

11. Организация сегмента телекоммуникаций специального назначения, обеспечивающего возможность электронного обмена специальными государственными органами сведениями, содержащими государственную тайну;

12. Разработка средств информационной безопасности, систем обеспечения безопасности операций с электронными документами, системы контроля действий государственных служащих при работе с информацией, разработка и совершенствование средств обработки информации общего пользования, систем удостоверяющих центров в сфере электронных цифровых подписей, а также системы сертификации и аудита.

Автор отмечает, что среди общих превентивных мер, направленных на предотвращение киберпреступности, приоритетными являются следующие:

– Более широкое использование возможностей индивидуальной и корпоративной защиты;

– Законодательный запрет на доступ в Интернет сети (или отдельные компьютеры) объектов государственной важности (атомные электростанции, оборонные предприятия); и развитие административных сетей, отдельных от общедоступных;

– Законодательный запрет на использование коммерческого программного обеспечения без исходного кода в области обработки конфиденциальной информации;

– Усиление доминирующего положения производителей программного обеспечения при покупке программного обеспечения государственными организациями на законодательном уровне.

При решении вопросов предотвращения киберпреступности, профилактические мероприятия направлены на создание благоприятных условий. Автор придерживается подхода, подтверждённого как отечественными, так и зарубежными экспертами, которые считают, что предотвратить киберпреступность всегда легче и проще, чем ее обнаружить и расследовать.

ЗАКЛЮЧЕНИЕ

На основе обобщения научного анализа и исследования теоретических и практических проблем уголовно-правовых и криминологических вопросов противодействия киберпреступности автор приходит к следующим выводам:

1. Эволюция компьютерных вирусов как основного фактора формирования киберпреступлений включает следующие этапы: 1970-1980-е годы; 1980-1992 годы; 1992-2000 гг.; 2000 г. – по настоящее время [13-А].

2. Формирование информативных технологий, а также их использование во всех сферах жизни человека приводит к появлению новых форм к киберпреступлений. Это обуславливает потребность принятия мер противодействия и совершенствования действующего уголовного законодательства и принятия новых норм [31-А].

3. На основе результатов существующего анализа определено понятие киберпреступления [12-А].

4. Киберпреступления классифицируются: а) в зависимости от объекта преступного посягательства; б) по характеру ущерба, причиненного компьютерной информации; в) в зависимости от способов совершения преступления [10-А]; [2-А].

5. Конвенция Европейского Союза о киберпреступности признана единственной конвенцией, признающей международное сотрудничество в борьбе с киберпреступностью [15-А].

6. Этапы международного сотрудничества Республики Таджикистан в обеспечении информационной безопасности от кибератак: 1992-2000 гг.; с 2001 года [16-А]; [27-А].

7. Из анализа законодательства иностранных государств выясняется, что составная структура и место киберпреступности в системе уголовного законодательства иностранных государств рассматриваются в различных формах [6-А]; [20-А].

8. Объектом преступлений против сетей Интернет и их вспомогательного оборудования являются общественные отношения в области преступлений против информационной безопасности, действий человека, различных личных и общественных интересов, а также охраняемых законом прав и интересов граждан [25-А]; [2-А].

9. Непосредственным объектом преступлений против сетей Интернет и их вспомогательного оборудования являются общественные отношения, которые в результате их совершения нарушают правовую систему доступа, использования и распространения компьютерной информации, право собственности на компьютерную систему, неприкосновенность компьютерной информации (программного обеспечения), безопасного использования компьютеров, электронной и компьютерной информации и нормальной работы компьютеров, сетей Интернет, а также безопасности использования интеллектуальных и материальных элементов вычислительных машин [2-А].

10 Объективной стороной преступлений против сетей Интернет и поддерживающего их оборудования являются внешние человеческие отноше-

ния, которые в целом можно разделить на две группы: 1) атаки, направленные на нарушение работы сетей связи и маршрутизаторов; 2) атаки, направленные на дополнение ресурсов операционной системы или программы [25-А]; [2-А].

11. В перечень объектов преступлений, совершенных с использованием различных технических средств, входят: конституционные права и свободы человека и гражданина (честь, достоинство и репутация человека, тайна личной жизни, личная и семейная тайна; тайна переписки). , телефонные переговоры, почтово-телеграфные письма, авторские и смежные права); компьютерная информация и информационные технологии; безопасность в области экономики, государственного управления, жизни и здоровья и общественной морали.

12. Объективная сторона преступлений, совершаемых различными техническими средствами, составляет внешние отношения лица по незаконному сбору и распространению информации о другом лице, или публичному отображению этих сведений в средствах массовой информации, а также к отправке электронных писем путем обмана через интернет – сеть. При совершении преступлений ставятся под угрозу права и законные интересы граждан [29-А].

13. Субъективная сторона преступлений, совершаемых посредством различными технических средств, может иметь место только по вине в виде прямого умысла [21-А].

14. Перечень субъектов, преступлений совершенных с использованием различных технических средств, обычно может быть общим, то есть физическое лицо, достигшее возраста, установленного уголовным законодательством. Но условно их можно разделить на две группы: 1) лица, обладающие специальными знаниями в области ИКТ и программирования (провайдеры, хакеры, операторы, программисты и т.п.); 2) обычные граждане. Преступления такого рода могут совершаться людьми, знакомыми с деятельностью Интернета и использующими его ежедневно. В целом для признания субъектом данных преступлений важно, чтобы лицо не было сотрудником той или иной организации или учреждения, а было обычным пользователем сетями Интернет [29-А].

15. В результате рассмотрения статистических данных и расследования уголовных дел, связанных с криминологическими вопросами киберпреступлений, необходимо прийти к следующему итоговому выводу:

– одной из основных тенденций развития киберпреступности является ее несвоевременное обнаружение. Этому процессу способствуют процессы незаконного создания информационно-коммуникационных сетей, мессенджеров и Интернета. Использование новых технологий в финансовых и кредитных операциях, онлайн-бизнесе, шифровании данных и т. д. не позволяет государству и обществу вовремя предотвратить большое количество киберпреступлений, поскольку они игнорируются по технологическим причинам.

– незнание жертвами киберпреступлений основных средств и методов защиты своей информации, позволяет злоумышленнику легко совершать противоправные действия. В связи с этим, важно отразить в средствах массовой информации наиболее распространенные планы киберпреступлений и способы их предотвращения, а также развивать у населения навыки обработки компьютерной информации и обучение работе с различными техническими устройствами, в том числе с сетью Интернет.

– высокий уровень киберпреступности во многом связан со сложностью выявления киберпреступной деятельности и нежеланием жертвы информировать правоохранительные органы [28-А].

– киберпреступники обладают обширными знаниями в области использования сети Интернет, различных технических средств и разработки вредоносных программ. Поэтому борьба с киберпреступностью должна осуществляться с привлечением специалистов, изучивших эти особенности.

– реальный объем и характер кибератак не в полной мере отражены в Центральном информационно-аналитическом центре МВД Республики Таджикистан.

– большинство жертв киберпреступлений – юридические лица. В связи с этим предприятиям и организациям необходимо уделить серьезное внимание обеспечению компьютерной безопасности от кибератак, определить в плане работы обязанности специалистов, принять меры по предотвращению любых кибератак с использованием современных технологий.

– самая большая угроза безопасности защищаемой компьютерной информации исходит от внутренних пользователей информационной системы. В связи с этим, особое значение имеет повышение профессионального уровня специалистов и мониторинг их надежности службой безопасности соответствующих органов.

16. Основными уголовно-правовыми факторами защиты ИКТ от преступных действий являются: на законодательно уровне должны быть отражены технологически новые способы совершения противоправных действий с использованием кибертехнологий и их возможные последствия, особенно противоправные действия против киберфизических систем, такие как перехват контрольных и подстрекательство к разведке, повреждение медицинского оборудования с помощью компьютерной атаки, повреждение систем жизнеобеспечения; основное внимание следует сосредоточить на процессе внедрения стратегий и принципов активного противодействия киберпреступности, в целях обеспечения благоприятных условий для борьбы с такими опасными для общества действиями со стороны правоохранительных органов; надлежащее межведомственное взаимодействие правоохранительной системы при проведении финансовых проверок, предотвращении всех форм мошенничества и хищения денежных средств, а также налаживании взаимовыгодного международного сотрудничества этих органов; разработка программ или стратегий как комплекса профилактических мер, подготовка соответствующей системы правоохранительных органов по борьбе с этими преступ-

лениями, а также рассмотрение вопроса защиты детей от любого рода агрессии, совершаемой через сети Интернет [22-А]; [28-А].

17. Потому как информативные технологические процессы в нынешний период никак не имеют конкретно установленного месторасположения, в данном случае преступники используют посторонние данные с любого участка. В связи с этим, автор считает необходимым предпринять следующие меры:

На национальном уровне:

– участие государства в разработке международной стратегии по противодействию киберугрозам, а также организации единого международно-правового механизма в киберпространстве;

– разработка проекта Государственной концепции либо Общегосударственной стратегии обеспечения кибербезопасности, базирующейся на принципах, а также нормах законодательства, реализация которых должна быть осуществлена на разных уровнях и сферах государства.

– разработка и внедрение многоуровневой институциональной системы кибербезопасности, охватывающей следующие факторы: 1) научно-аналитический уровень, согласно которому киберриски изучаются в связи с вероятностью возникновения киберугроз и масштабных негативных последствий; 2) практический урован, скоординированный в двух направлениях – внутреннем (межнациональными органами, отвечающими из-за обнаружение а также сопротивление киберугрозам) а также внешнем – осуществляется в рамках координации национальных организаций а также областных и интернациональных институтов;

– повышение потенциала информационного сектора по борьбе с кибератаками, что усиливает внутриполитические меры, связанные с технологиями кибербезопасности;

– охрана (т.е. сотрудничество в области наблюдения за деятельностью работы незаконных, террористических формирований, функционирующих в киберпространстве) посредством реализации регионального и международного сотрудничества;

– совершенствование интернационального партнерства подразумевает привлечение к деятельности по борьбе с киберпреступностью различных структур, нацеленных на искоренение киберугроз.

На международном уровне:

– разработка международных соглашений в области противодействия киберугрозам между таджикистаном и зарубежными странами.

– создание международного института с региональными представительствами. Этот институт должен быть частью ООН в виртуальном пространстве и включать в себя несколько структур, например, принимать программы или концепции в этом направлении, разрабатывать планы, реализовывать задачи, которые должны быть унифицированы на государственном уровне и т.д. [9-А].

Рекомендации по практическому использованию результатов исследования

1. Необходимо принять образовательные программы и государственные стандарты в направлении обеспечения безопасности информации от кибератак [17-А]; [18-А].

2. В рамках высших учебных заведений страны должна быть введена специальность «кибербезопасность» [30-А].

3. Работа Совета по информационно-коммуникационным технологиям при Президенте Республики Таджикистан была обновлена и сформирована другими советами, направленными на то, чтобы передать ему функции координации и межотраслевого руководства субъектами борьбы с киберпреступностью (в том числе Генеральной прокуратурой РТ, КГБ РТ, МВД РТ и Министерства юстиции РТ).

4. Принимая во внимание сложную и тревожную ситуацию в регионе и мире, а также сбор и обработку информации о киберпреступлениях, проведение экспертной оценки киберугроз, разработку и внедрение передовых методов предотвращения и расследования киберпреступлений, в рамках ОДКБ создать в качестве специализированного органа «Центр по борьбе с киберпреступностью» [24-А].

5. Единый коммутативный центр электросвязи Службы связи при Правительстве РТ, Генеральная Прокуратура РТ и Министерство внутренних дел РТ должны ограничить доступ к веб-сайтам и другим информационным ресурсам (включая веб-сайт и интернет-программы, направленные на распространение любой информации против основ конституционного строя, личной, общественной, государственной безопасности, снижения национального достоинства).

6. Для получения нормативно-правового статуса понятий киберпреступлений, кибербезопасности, киберпространства, объекта информации, киберугроз, объекта кибербезопасности, субъекта обеспечения кибербезопасности, кибератак, единой государственной политики в области кибербезопасности, уполномоченного государственного органа в области кибербезопасности, прав и обязанностей уполномоченных государственных органов в области кибербезопасности, системы обеспечения кибербезопасности, научно-технической и инновационной поддержки в области кибербезопасности в области кибербезопасности, должны принять Закон Республики Таджикистан «О кибербезопасности» [26-А].

7. В целях совершенствования уголовного законодательства и усиления факторов противодействия киберпреступлениям необходимо внести изменения в Уголовный кодекс Республики Таджикистан. В частности, в главу 28 УК РТ считаем необходимым внести следующие предложения, связанные с внесением изменений и дополнений в уголовное законодательство:

а) статья 298 (1). Получение персональной электронной информации путем мошенничества или иными способами незаконного доступа к информации в корыстных целях;

б) статью 300 Уголовного кодекса Республики Таджикистан дополнить в новой редакции частью 2;

в) статья 300 (1) Компьютерная атака DoS и статья 301 (2) главы 28 Уголовного кодекса. Незаконное распространение электронных писем в виде новых статей;

г) целесообразно дополнить часть 3 статьи 301 УК РТ отдельными пунктами;

д) статья 301 (3). Разработка, публикация и распространение информации с использованием сети Интернет и любых средств информационных и телекоммуникационных сетей будут входить в состав Республики Таджикистан;

е) имеется необходимость внесения изменений в часть 2 статьи 302 Уголовного кодекса Республики Таджикистан;

ё) статью 303 Уголовного кодекса Республики Таджикистан предлагается изложить в новой редакции: статью 303. Незаконная разработка, использование или распространение вредоносных компьютерных программ.

8. На основании рассмотрения и анализа объекта преступлений против сетей Интернет и их вспомогательного оборудования считаем целесообразным ввести в Уголовный кодекс РТ раздел под названием «Преступления против кибербезопасности» [25-А].

ПЕРЕЧЕНЬ
НАУЧНЫХ ПУБЛИКАЦИЙ СОИСКАТЕЛЯ УЧЕНОЙ СТЕПЕНИ

I. Монографии:

[1-А]. Раджабов, К.Д. Уголовно-правовые и криминологические проблемы борьбы с вымогательством [Текст]: монография / К.Д. Раджабов. – Душанбе: «Лахути», 2020. – 156 с. (9,75 п.л.); ISBN 978-99975-358-7-0.

[2-А]. Давлатзода, К.Д. Таҳдидҳои фазои маҷозӣ: амалия ва назарияи киберҷиноятҳо [Матн]: монография / К.Д. Давлатзода. – Душанбе: «Матбааи ДМТ», 2023. – 248 с. (15,5 ч.ч.); ISBN 978-99985-41-01-6.

II. Статьи, опубликованные в рецензируемых и рекомендованных Высшей аттестационной комиссией при Президенте Республики Таджикистан журналах:

[3-А]. Раджабов, К.Д. Развитие понятия вымогательства в уголовном праве [Текст] / К.Д. Раджабов // Вестник Таджикского национального университета. – 2017. – №2/7. – С. 237-241; ISSN 2413-5151.

[4-А]. Раджабов, К.Д. Объективная сторона вымогательства [Текст] / К.Д. Раджабов // Вестник Таджикского национального университета. – 2018. – №2. – С. 210-214; ISSN 2413-5151.

[5-А]. Давлатзода, К.Д. Масоили таърихӣ ва назариявии ташаккули ҷиноятҳои компютерӣ [Матн] / К.Д. Давлатзода // Қонунгузорӣ. – 2021. – №4 (44). – С. 92-95; ISSN 2410-2903.

[6-А]. Давлатзода, К.Д., Назаров, А.Қ. Таҳлили муқоисавии ҳуқуқи ҷиноятӣ дар самти мубориза бар зидди ҷиноятҳои компютерӣ дар кишварҳои

аъзои ИДМ ва дигар давлатҳои хориҷӣ [Матн] / К.Д. Давлатзода, А.Қ. Назаров // Паёми Донишгоҳи миллии Тоҷикистон. Бахши илмҳои иҷтимоӣ-иқтисодӣ ва ҷамъиятӣ. – 2022. – №3. – С. 229-236; ISSN 2413-5151.

[7-А]. Давлатзода, К.Д., Назаров, А.Қ. Истифодаи технологияи рақамӣ дар фаъолияти оперативӣ-ҷустуҷӯӣ [Матн] / К.Д. Давлатзода, А.Қ. Назаров // Паёми Донишгоҳи миллии Тоҷикистон. Бахши илмҳои иҷтимоӣ-иқтисодӣ ва ҷамъиятӣ. – 2022. – №4. – С. 207-212; ISSN 2413-5151.

[8-А]. Давлатзода, К.Д. Праблемаҳои ҳуқуқии-ҷиноятии мафҳуми ғайриқонунӣ ба даст овардани иттилооти компютерӣ [Матн] / К.Д. Давлатзода // Давлатшиносӣ ва ҳуқуқи инсон. – 2022. – №1 (25). – С. 179-187; ISSN 2414 9217.

[9-А]. Давлатзода, К.Д. Ҷаҳонишавии проблемаҳои киберҷиноятҳо [Матн] / К.Д. Давлатзода // Паёми Донишгоҳи миллии Тоҷикистон. Бахши илмҳои иҷтимоӣ-иқтисодӣ ва ҷамъиятӣ. – 2022. – №9. – С. 231-237; ISSN 2413-5151.

[10-А]. Давлатзода, К.Д. Таснифоти киберҷиноятҳо [Матн] / К.Д. Давлатзода // Паёми Донишгоҳи миллии Тоҷикистон. Бахши илмҳои иҷтимоӣ-иқтисодӣ ва ҷамъиятӣ. – 2022. – №8. – С. 279-284; ISSN 2413-5151.

[11-А]. Давлатзода, К.Д. Танзими ҳуқуқии муносибатҳо дар соҳаи иттилооти компютерӣ [Матн] / К.Д. Давлатзода // Қонунгузорӣ. – 2022. – №2 (46). – С. 117-122; ISSN 2410-2903.

[12-А]. Давлатзода, К.Д. Таҳқиқоти ҳуқуқии ҷиноятии мафҳуми киберҷиноятҳо [Матн] / К.Д. Давлатзода // Давлатшиносӣ ва ҳуқуқи инсон. – 2022. – №3 (27). – С. 428-434; ISSN 2414 9217.

[13-А]. Давлатзода, К.Д. Таҳаввулоти вирусҳои компютерӣ ҳамчун омили асосии пайдоиш ва содишавии киберҷиноятҳо [Матн] / К.Д. Давлатзода // Паёми Донишгоҳи давлатии Данғара. – 2022. – №4 (22). – С. 138-144; ISSN 2410-4221.

[14-А]. Давлатзода, К.Д. Кибертерроризм ҳамчун намуди нави амали террористӣ [Матн] / К.Д. Давлатзода // Паёми Донишгоҳи миллии Тоҷикистон. Бахши илмҳои иҷтимоӣ-иқтисодӣ ва ҷамъиятӣ. – 2023. – №1. – С. 207-213; ISSN 2413-5151.

[15-А]. Давлатзода, К.Д. Аҳаммияти санадҳои байналмилалӣ дар муқовимат бо киберҷиноятҳо [Матн] / К.Д. Давлатзода // Паёми Донишгоҳи миллии Тоҷикистон. Бахши илмҳои иҷтимоӣ-иқтисодӣ ва ҷамъиятӣ. – 2023. – №2. – С. 221-229; ISSN 2413-5151.

[16-А]. Давлатзода, К.Д. Ҳамкориҳои минтақавии Ҷумҳурии Тоҷикистон дар самти мубориза бо киберҷиноятҳо: дар мисоли Созмони ҳамкории Шанхай ва Созмони паймони амнияти дастаҷамъӣ [Матн] / К.Д. Давлатзода // Паёми Донишгоҳи миллии Тоҷикистон. Бахши илмҳои иҷтимоӣ-иқтисодӣ ва ҷамъиятӣ. – 2023. – №6. – С. 232-237; ISSN 2413-5151.

[17-А]. Давлатзода, К.Д. Тавсифи ҳуқуқии ҷиноятии савдои одамон дар фазои киберӣ [Матн] / К.Д. Давлатзода // Паёми Донишгоҳи миллии

Тоҷикистон. Бахши илмҳои иҷтимоӣ-иқтисодӣ ва ҷамъиятӣ. – 2023. – №8. – С. 228-234; ISSN 2413-5151.

[18-А]. Давлатзода, К.Д. Порнографияи кӯдакон дар Интернет: мафҳум, оқибат ва масъалаҳои ҳуқуқии ҷиноятии муборизаи бар зидди он [Матн] / К.Д. Давлатзода // Паёми Донишгоҳи миллии Тоҷикистон. Бахши илмҳои иҷтимоӣ-иқтисодӣ ва ҷамъиятӣ. – 2023. – №9. – С. 244-249; ISSN 2413-5151.

[19-А]. Давлатзода, К.Д. Тамаъҷӯӣ дар фазои маҷозӣ: мафҳум ва хусусиятҳои он [Матн] / К.Д. Давлатзода // Қонунгузорӣ. – 2023. – №3 (51). – С. 144-150; ISSN 2410-2903.

[20-А]. Давлатзода, К.Д. Ҷавобгарии ҷиноятӣ барои киберҷиноятҳо тибқи қонунгузории Ҷумҳурии Мардумии Чин: таҳлили муқоисавии ҳуқуқӣ [Матн] / К.Д. Давлатзода // Осори Академияи ВКД Ҷумҳурии Тоҷикистон. – 2023. – №3 (59). – С. 31-36; ISSN 2412-141X.

[21-А]. Давлатзода, К.Д. Нишонаҳои тарафи субъективии ҷиноятҳо ба муқобили шабакаҳои интернетӣ ва таҳҳизотҳои ёрирасони онҳо ҳамчун намуди нави киберҷиноятҳо (барномаҳои зараровар ва ҳамлаҳои DoS) [Матн] / К.Д. Давлатзода // Паёми Донишгоҳи миллии Тоҷикистон. Бахши илмҳои иҷтимоӣ-иқтисодӣ ва ҷамъиятӣ. – 2023. – №10. – С. 233-240; ISSN 2413-5151.

[22-А]. Давлатзода, К.Д. Тавсифи криминалогии шахсияти киберҷинояткор [Матн] / К.Д. Давлатзода // Қонунгузорӣ. – 2023. – №4 (51). – С. 211-217; ISSN 2410-2903.

III. Научные статьи, опубликованные в сборниках и других научно-практических изданиях:

[23-А]. Давлатзода, К.Д., Назаров, А.Қ. Нақши тафаккури сунъӣ дар раванди амалишавии фаъолияти оперативӣ-ҷустуҷӯӣ [Матн] / К.Д. Давлатзода, А.Қ. Назаров // Криминалистикаи муосир: маводи конференсияи ҷумҳуриявии илмӣ-амалӣ // Зери назари умумии н.и.ҳ., дотсент Ф.Р. Шарифзода. – Душанбе: Нашриёти ВКД Ҷумҳурии Тоҷикистон, 2022. – С. 111-117.

[24-А]. Давлатзода, К.Д., Назаров, А.Қ. Ташкилотҳои байналмилалӣ ҳамчун субъектони муқовимат бо киберҷиноятҳо [Матн] / К.Д. Давлатзода, А.Қ. Назаров // Маводи конференсияи байналмилалии илмӣ-амалӣ бахшида ба 25-солагии Кодекси ҷиноятии Ҷумҳурии Тоҷикистон: ҳолат ва дурнамо. – Душанбе: Нашриёти ВКД Ҷумҳурии Тоҷикистон, 2023. – С. 143-148.

[25-А]. Давлатзода, К.Д. Барномаҳои зараровар ҳамчун воситаи содиршавии киберҷиноятҳо: мафҳум ва намудҳои он [Матн] / К.Д. Давлатзода // Маҷмуи мақолаҳои конференсияи ҷумҳуриявии илмию-амалӣ дар мавзуи «Мушкилотҳои қонунгузории замин дар даврони муосир». – Душанбе, 2023. – С. 235-238.

[26-А]. Давлатзода, К.Д. Таҳдидҳои киберӣ: қаллобӣ дар фазои маҷозӣ [Матн] / К.Д. Давлатзода // Маҷмуи мақолаҳои конференсияи байналмилалӣ дар мавзуи «Тоҷикон дар оинаи таърих», бахшида ба 115 солагии академик Бобоҷон Ғафуров (Филиали Донишгоҳи давлатии Москва ба номи Михаил Ломоносов дар шаҳри Душанбе). – Душанбе, 2023. – С. 61-64.

[27-А]. Давлатзода, К.Д. Ташаббусҳои байналмилалии Ҷумҳурии Тоҷикистон дар таъмини амнияти иттилоотӣ аз ҳамлаҳои киберӣ [Матн] / К.Д. Давлатзода // Маводи конференсияи байналмилалии илмию амалии «Илм ва таҳсилот: тамоюлҳои рушд дар ҷомеаи иттилоотӣ» бахшида ба «75-солагии ДМТ». – Душанбе, 2023. – С. 405-409.

[28-А]. Давлатзода, К.Д. Хакер: тавсифи криминологии он [Матн] / К.Д. Давлатзода // Масоили мубрами такмили Конститутсияи Ҷумҳурии Тоҷикистон дар шароити муосир: маводи конференсияи ҷумҳурявии илмию назариявӣ бахшида ба 75-солагии Донишгоҳи миллии Тоҷикистон. – Душанбе, 2023. – С. 227-233.

[29-А]. Давлатзода, К.Д. Интернет воситаи содиршавии кибертаъқиб [Матн] / К.Д. Давлатзода // Ҳифзи ҳуқуқи инсон ва масъалаи муқовимат ба коррупсия дар ҷаҳони муосир: консепсияҳо, воқеият ва дурнамо: маводи конференсияи байналмилалии илмӣ-амалӣ бахшида ба 75-умин солгарди қабули Эъломияи умумии ҳуқуқи инсон ва рӯзи байналмилалии мубориза бар зидди коррупсия (Академияи идоракунии давлатии назди Президенти ҶТ). – Душанбе, 2023. – С. 189-169.

[30-А]. Давлатзода, К.Д. Таҳлили таҷрибаи амалии мақомоти ваколатдори давлатӣ ва ҳамкории байналмилалии онҳо дар самти таъмини амнияти киберӣ [Матн] / К.Д. Давлатзода // Масъалаҳои назариявии ташаккули фарҳанги ҳуқуқи инсон дар Тоҷикистон: маводи конференсияи байналмилалии илмию назариявӣ. – Душанбе, 2023. – С. 280-289.

IV. Методические пособия:

[31-А]. Давлатзода, К.Д. Асосҳои тафтиши киберҷиноятҳо [Матн]: воситаи таълимӣ / К.Д. Давлатзода. – Душанбе: «Матбааи ДМТ», 2023. – 150 с. (9,3 ҷ.ч.); – ISBN 978-99985-41-11-5.

ФИШУРДА

ба диссертатсияи Давлатзода Комрон Давлат дар мавзуи «Масъалаҳои ҳуқуқӣ-ҷиноятӣ ва криминологии муқовимат бо киберҷиноятҳо: проблемаҳои назариявӣ ва амалӣ»

Калидвожаҳо: киберҷиноятҳо, ҳамлаҳои киберӣ, ҷавобгарии ҷиноятӣ, ҳуқуқи ҷиноятӣ, қонунгузории ҷиноятӣ, давлатҳои пасошуравӣ, ҳамкории байналмилалӣ, созмонҳои байналмилалӣ, технологияҳои иттилоотию коммуникатсионӣ, интернет, барномаҳои зараровар, ҳамлаҳои DoS, мактубҳои фишингӣ, кибертаъқиб, дуздии онлайнӣ.

Мақсади таҳқиқоти диссертатсионӣ таҳқиқи маҷмуии масъалаҳои ҳуқуқӣ-ҷиноятӣ ва криминологии муқовимат бо киберҷиноятҳо: проблемаҳои назариявӣ ва амалӣ, ошкор намудани ҳама намудҳои ин гуна ҳамкорӣ дар муқовимат бо ин кирдори барои ҷамъият хавфнок, таҳқиқи ҷавобгарии ҷинояти барои киберҷиноятҳо ва тафриқагузории он дар низоми қонунгузории давлатҳои хориҷӣ, таҳлили таркиби ин ҷиноятҳо вобаста ба аломатҳои объективӣ ва субъективӣ, инчунин тавсифи криминологии киберҷиноятҳост.

Дар ҷараёни таҳқиқ методҳои диалектикӣ, расмӣ-ҳуқуқӣ, расмӣ-мантиқӣ, муқоисави-ҳуқуқӣ, оморӣ ва дигар методҳои умумӣ ва махсуси илмӣ, ки ҷониби илм таҳия ва дар амалия санҷидашудаанд, истифода шудаанд. Методҳои умумӣ-илмӣ имкон дод, ки омӯзиши нақши технологияҳои иттилоотӣ-коммуникатсионӣ, дар рушди ҷомеа ва таъсири онҳо ба ҷомеаи муосир, истифодаи бемавриди онҳо дар шароити ҷаҳонишавӣ чӣ паёмадҳо дорад. Методологияи дар таҳқиқ истифодашуда шароит фароҳам овард, ки он ҳамаҷониба анҷом ёфта, пайдоиши падидаҳо ва зерпадидаҳои нав муайян карда шавад, инчунин тамоюлҳои нави ҳамкориҳои байналмилалӣ дар муқовимат бо киберҷиноятҳо муайян карда шаванд ва идеяҳои нав ҷиҳати самаранок амалӣ сохтани онҳо дар таҷриба пешниҳод карда шаванд.

Навгонии илмии таҳқиқ аз он иборат аст, ки бори аввал таҳқиқоти диссертатсионии ватанӣ дар самти масъалаҳои ҳуқуқӣ-ҷиноятӣ ва криминологии муқовимат бо киберҷиноятҳо: проблемаҳои назариявӣ ба таври комплексӣ омӯхта шуда, мазмуни ҳамкории байналмилалӣ, ва роҳҳои ҳамоҳангсозии муқовимат бо он дар қонунгузорӣ ва амалияи татбиқи он, таҳлили таркиби ин ҷиноятҳо вобаста ба аломатҳои объективӣ ва субъективӣ муқаррароти нав мебошанд. Зеро дар миқёси ҷаҳонӣ то ҳол механизми ягонаи байналмилалии ҳуқуқӣ-ҷиноятӣ, криминологии муқовимат бо киберҷиноятҳо ва истилоҳоти ягона таҳия нагардида буд, ки ин омил, ҳамкории давлатҳоро дар ин самт мушкил месохт.

Бо мақсади такмили қонунгузории ҷиноятӣ ва мустаҳкам гардонидани омилҳои муқовимат бо киберҷиноятҳо дар рисола пешниҳод карда шудааст, ки дар боби 28 КҶ ҶТ КҶ ҶТ тағйиру иловаҳо ворид карда шаванд: ба моддаи 298 (1); қ. 2 м. 300; м. 300 (1) ; м. 301 (2); қ. 3 м. 301; м. 301 (3); қ. 2 м. 302; м. 303 КҶ ҶТ.

АННОТАЦИЯ

на диссертацию Давлатзода Комрона Давлата на тему «Уголовно-правовые и криминологические вопросы противодействия киберпреступности: теоретические и практические проблемы»

Ключевые слова: киберпреступность, кибератаки, уголовная ответственность, уголовное право, уголовное законодательство, постсоветские государства, международное сотрудничество, международные организации, информационно-коммуникационные технологии, интернет, вредоносные программы, DoS-атаки, фишинговые письма, кибersталкинг, кража онлайн-личности.

Целью диссертационного исследования является комплексное исследование теоретических и практических уголовно-правовых и криминологических вопросов противодействия киберпреступности, выявление всех видов такого взаимодействия в противодействии этому общественно-опасному деянию, иследование уголовной ответственности за киберпреступность и ее дифференциация в системе законодательства зарубежных государств, анализ состава этих преступлений, связанных объективными и субъективными признаками, а также криминологическое описание киберпреступности.

В ходе исследования использовались диалектические, формально-правовые, формально-логические, сравнительно-правовые, статистические и другие общие и специальные научные методы, разработанные наукой и проверенные на практике. Общенаучные методы позволили изучить роль информационно-коммуникационных технологий в развитии общества и определить уровень их влияния на современное общество, выявить последствия их нецелевого использования в условиях глобализации. Методология, используемая в исследовании, создала условия для того, чтобы она была исчерпывающей и определяла появление новых явлений и субподрядов, а также выявила новые тенденции международного сотрудничества в противодействии киберпреступности, предложив новые идеи для эффективного их осуществления на практике.

Научная новизна исследования заключается в том, что впервые отечественном диссертационном исследования комплексно изучаются теоретические и практические проблемы уголовно-правовых и криминологических вопросов противодействия киберпреступности. Содержание международного сотрудничества, и способы согласования с ним сравнений в законодательстве и практике его применения, анализ состава этих преступлений являются новыми положениями в зависимости от объективных и субъективных признаков. В глобальном масштабе до сих пор не был разработан единый международный уголовно-правовой, криминологический механизм противодействия киберпреступности и единая терминология, что затрудняет взаимодействие государств в этом направлении.

В целях совершенствования уголовного законодательства и усиления факторов противодействия киберпреступлениям в диссертации предлагается внести изменения и дополнения в главу 28 УК РТ: в статью 298(1); ч. 2 ст. 300; ст. 300 (1); статья 301 (2); ч. 3 ст. 301; статья 301 (3); ч. 2 ст. 302; ст. 303 УК РТ.

ANNOTATION

On the dissertation of Davlatzoda Komron Davlat to the topic «Criminal-legal and criminological issues of counteraction to cybercrime: theoretical and practical problems».

Keywords: cybercrimes, cyberattacks, criminal liability, criminal law, criminal legislation, post-Soviet states, international cooperation, international organizations, information and communication technologies, Internet, malware, DoS attacks, phishing emails, cyberstalking, online identity theft.

The purpose of the dissertation research is a comprehensive study of theoretical and practical criminal-legal and criminological issues of countering cybercrime, identification of all types of such interaction in countering this socially dangerous act, research of criminal liability for cybercrime and its differentiation in the system of legislation of foreign countries, analysis of the composition of these crimes related to objective and subjective features, as well as the criminological description of cybercrimes.

During the research dialectical, formal-legal, formal-logical, comparative-legal, statistical and other general and special scientific methods developed by science and tested in practice were used. General scientific methods made it possible to study the role of information and communication technologies in the development of society and to determine the level of their influence on modern society, to identify the consequences of their misuse in the conditions of globalization. The methodology used in the research created the conditions for it to be exhaustive and to identify the emergence of new phenomena and sub institutes, as well as to identify new trends in international cooperation in countering cybercrime, offering new ideas for their effective implementation in practice.

Scientific novelty of the research is expressed in that, it is the first domestic dissertation research that comprehensively studied theoretical and practical problems of criminal-legal and criminological issues of counteraction to cybercrime. The content of international cooperation, and ways to harmonize with it comparisons in the legislation and practice of its application, the analysis of the composition of these crimes are new provisions depending on the objective and subjective features. Globally, a unified international criminal and criminological mechanism for countering cybercrime and a common terminology have not yet been developed, which makes it difficult for States to cooperate in this area.

In order to improve criminal legislation and strengthen the factors of counteraction to cybercrime, the dissertation proposes to make amendments and additions to Chapter 28 of the Criminal Code of the RT: Article 298(1); Part 2, Art. 300; Art. 300 (1); Art. 301 (2); Part. 3 of Art. 301; Art. 301 (3); Part 2 of Art. 302; Art. 303 of the Criminal Code of the Republic of Tajikistan.

Ба чоп __.04.2024 иҷозат дода шуд. Андозаи 60x84 1/16.
Коғази офсет. Чопи офсет. Гарнитураи Times New Roman Tj.
Ҷузъи чопии шартӣ 7,0.
Теъдоди нашр ___ нусха. Супориши № ___.