КОМПЬЮТЕР АХБОРОТИНИ МОДИФИКАЦИЯЛАШТИРИШ ЖИНОЯТИНИНГ ЮРИДИК-ТЕХНИК ТАҲЛИЛИ ВА УШБУ ҚИЛМИШ УЧУН ЖАЗО МУҚАРРАРЛИГИНИ ТАЪМИНЛАШ МЕХАНИЗМИ

Анорбоев Амириддин Улуғбек ўғли, ю.ф.д.
https://orcid.org/0009-0003-5355-8753
e-mail: a.anorboyev786@mail.ru

Аннотация: *Мазкур мақолада Ўзбекистон Республикаси Жиноят кодексининг 278[4]-моддасида назарда тутилган компьютер ахборотини модификациялаштириш жиноятининг юридик-техник муаммолари комплекс таҳлил қилинган. Тадқиқотда ҳуқуқий ва технологик мезонларни бирлаштирувчи инновацион "кибералогия" методи асосида жиноят таркибининг элементлари, рақамли излар тизими ва зарур суд экспертизалари классификацияси ишлаб чиқилган.*

Калит сўзлар*: кибержиноятчилик, кибералогия методи, Жиноят кодекси 278[4]-моддаси, ахборот яхлитлиги, маълумотларни заҳарлаш, рақамли излар, муҳим ахборот инфратузилмаси, инсайдерлик таҳдидлари, IT соҳасида ишлаш ҳуқуқидан маҳрум қилиш.*

Ўзбекистон Республикаси Жиноят кодексининг 278[4]-моддасига асосан, компьютер ахборотини модификациялаштириш, яъни компьютер тизимида сақланаётган ахборотни қонунга хилоф равишда ўзгартириш, унга шикаст етказиш, уни ўчириш, худди шунингдек била туриб унга ёлғон ахборотни киритиш фуқароларнинг ҳуқуқларига ёки қонун билан қўриқланадиган манфаатларига ёхуд давлат ёки жамоат манфаатларига кўп миқдорда зарар ёхуд жиддий зиён етказилишига сабаб бўлиши[1]

жиноий жавобгарликка сабаб бўлади ва ушбу жиноятни кибералогия методи асосида юридик-техник таҳлил қилинганида қуйидаги муаммолар аниқланди, хусусан:

1) жиноят моддаси номи ва диспозициясида назарда тутилган "**компьютер ахбороти ва компьютер тизими**" тушунчалари жуда тор бўлиб, ахборот-коммуникация технологияларининг кейинги ривожига асосан, компьютер тизими ҳисобланмайдиган бошқа ахборот тизимлари ёки мазкур тизимлардаги ахборотни ҳам ушбу тизимга киритиш билан боғлиқ жиддий технологик муаммо мавжуд. Бу эса, компьютер тизими ва компьютер ахборотига оид бўлмаган воситалар билан боғлиқ қилмиш ЖКнинг 278^4-моддасида назарда тутилган тартибда содир этилиши айбдор шахсга нисбатан жазо қўлланилиши ўз навбатида ҳеч ким суднинг ҳукми бўлмай туриб жиноят содир қилишда айбли деб топилиши ва қонунга хилоф равишда жазога тортилиши мумкин эмаслиги ҳақидаги принципга зид саналади.

Маълумот учун: Германияда *жиноят қонунчилигига кўра, компьютер ахборотининг ўрнига ҳар қандай электрон, магнит ёки бошқа кўринмас шаклда сақланувчи, устидан бошқа шахс тасарруф этиш ҳуқуқига эга бўлган маълумотлар тушунчаси қўлланилади[2],* ***АҚШ****да "муҳофаза этиладиган компьютер" тушунчаси штатлараро ёки халқаро тижорат ва алоқада фойдаланиладиган ҳар қандай қурилмани, шу жумладан виртуал булутли серверлар ва IoT қурилмаларини ўз ичига олади[3],* ***Буюк Британия****да "компьютер" ва "дастур" тушунчалари технологиядан мустақил равишда таърифланган бўлиб, унга кўра марказлашмаган блокчейн тармоқлари ва улардаги смарт-контрактлар ҳам ҳимоя объекти ҳисобланади[4].* ***Франция****да "автоматлаштирилган маълумотларни қайта ишлаш тизими" (STAD) тушунчасини қўллайди. Кассация судининг*

прецедентларига кўра, ушбу тушунча остига тармоққа уланган ҳар қандай смарт-қурилмалар ва сунъий интеллект платформалари киритилган[5], ***Сингапурда*** *компьютер тушунчасини шундай кенг таърифлайдики, у маълумотларга ишлов берувчи ҳар қандай юқори технологик қурилмани, жумладан сунъий интеллектнинг нейротармоқларини қамраб олади[6],* ***Австралияда*** *"электрон алоқа воситасида сақланувчи маълумотлар" ибораси қўлланган бўлиб, бу маълумотнинг жисмоний компьютерда ёки масофавий булутли инфратузилмада эканлигидан қатъи назар бир хил ҳимояланишини таъминлайди[7].* ***Канадада*** *"компьютер тизими" (computer system) тушунчасини маълумотларни қайта ишловчи ва ички хотирага эга қурилмалар мажмуи сифатида таърифлайди, бу эса саноатдаги IoT датчикларини автоматик равишда жиноят предметига айлантиради[8].* ***Эстонияда*** *компьютер тизими тушунчасини "рақамли маълумотларни қайта ишловчи тизимлар" деб беради ва ушбу давлатнинг рақамли реестрлари (X-Road) ва ундаги блокчейн технологияси ушбу модда билан қўриқланади[9].* ***Жанубий Кореяда*** *ахборот тармоқлари орқали узатиладиган ёки сақланадиган барча рақамли маълумотларнинг яхлитлигини булут технологиялари фонида кафолатлайди[10].* ***Японияда*** *"электрон қайдлар" (electronic records) устидан назоратни бузишни тақиқлайди, бу эса маълумотнинг жисмоний ташувчида эмас, балки виртуал серверлар ва сунъий интеллект моделларида жойлашишидан қатъи назар жиноий жавобгарликка сабаб бўлади[11];*

2) ЖКнинг 278^4-моддасида назарда тутилган компьютер тизимида сақланаётган ахборотни қонунга хилоф равишда ўзгартириш бу компьютер ахборотини модификациялаштириш ҳисобланади, бироқ ушбу ахборотга шикаст етказиш, уни ўчириш, худди шунингдек била

туриб унга ёлғон ахборотни киритиш том маънода амалдаги таҳрирга кўра, компьютер ахборотини ўзгартиришнинг таркибига кирмайди, қолаверса, компьютер ахбороти шикастланган бўлиши мумкин, бироқ файл ичидаги ахборот бошқа ресурсларда ўқиши мумкин. Масалан, компьютерга баъзан флешкадаги ахборотни ўқимай қолади, бироқ Total Commander дастурида флешка очилса, ундаги ахборот ўқилиши мумкин. Мазкур вазиятда, айбдорнинг ҳаракатларини ҳуқуқий ва технологик жиҳатдан тўғри малакалаш учун ушбу модданинг номи ва мазмунини ўзаро мувофиқлаштириш зарур.

Маълумот учун: Нидерландияда *маълумотларни ўзгартиришни (модификация) ва маълумотларни фойдаланиб бўлмайдиган ҳолатга келтиришни (шикастлаш) иккита алоҳида мустақил ҳаракат сифатида диспозицияда ажратиб кўрсатади[12].* ***Австрияда*** *маълумотларни ўчиришни (Löschen) ва уларни яроқсиз ҳолга келтиришни (Unbrauchbarmachen) модификациядан алоҳида жиноий ҳаракат сифатида квалификация қилади[13].* ***Швейцарияда*** *маълумотларни ўзгартириш, ўчириш ёки йўқ қилиш ҳаракатларини тизимли равишда "маълумотлар яхлитлигини бузиш" умумий тушунчаси остида, лекин ҳар бирининг техник чегарасини ажратган ҳолда баён этади[14].* ***Италияда*** *компьютер маълумотларини, дастурларини ва тизимларини бузиш, йўқ қилиш ёки ўзгартириш ҳаракатларини дифференциация қилади, бу эса терговга айбловни аниқ техник ҳаракат масалан, фақат ўчириш бўйича қўйиш имконини беради[15].* ***Испанияда*** *маълумотларга жиддий зарар етказиш, ўчириш ва уларни модификация қилишни алоҳида диспозиция элементлари сифатида кўради ва қалбаки маълумот киритиш (сохталаштириш) ҳаракатини ушбу моддадан чиқариб, компьютер сохтакорлиги (264bis) сифатида алоҳида баҳолайди[16].* ***Польшада*** *ахборотни йўқ қилиш, ўчириш ва ўзгартириш ҳаракатлари*

*билан бир қаторда, унга янги маълумот киритиш орқали тизим яхлитлигига тўсқинлик қилишни алоҳида банд билан тартибга солади[17]. **Данияда** маълумотларни ноқонуний модификация қилишни алоҳида, уларни бутунлай йўқ қилиб юборишни эса мулкка зарар етказишнинг махсус шакли сифатида баҳолаб, тизимлиликни таъминлаган[18]. **Норвегияда** маълумотларни модификация қилишни тизим ишини сезиларли даражада ўзгартирганлик учун, 203-моддасини эса ахборотни йўқ қилганлик (ўчирганлик) учун алоҳида жавобгарлик сифатида белгилайди[19];*

3) ЖКнинг 278^4-модданинг биринчи қисми диспозицияси технологик жиҳатдан эскирган бўлиб, фақат ўзгартириш, ўчириш, шикаст етказиш ва ёлғон киритиш ҳаракатлари эмас, балки шифрлаш, сунъий интеллект орқали ахборотни заҳарлаш, ахборотни монипуляция қилиш, конфигурация маълумотларини таҳрирлаш, overwrite, suppression каби замонавий ҳужумлар ҳам компьютер ахборотини модификациялаши мумкин.

***Маълумот учун**: **АҚШда** маълумотларни шифрлаш орқали улардан фойдаланишни тўсиб қўйишни (Ransomware ҳужумлари) тизимга зарарли буйруқ юбориш ва ундан фойдаланиш имкониятини чеклаш сифатида баҳолайди, бу эса моддий модификация бўлмаса ҳам жиноят ҳисобланади[20]. **Буюк Британияда** маълумотларни ўзгартирмасдан, фақат уларни вақтинча блокга солувчи (Suppression) ёки шифрловчи ҳужумларни тўлиқ қамраб олади[21]. **Сингапур** "Компьютерларни суиистеъмол қилиш тўғрисида"ги қонуннинг 5-моддаси тизимдаги маълумотларни сунъий равишда манипуляция қилишни тақиқлайди, бу эса СИ моделларининг ўқитиш базасини бузишга қаратилган маълумотларни заҳарлаш (data poisoning) ҳужумларини криминаллаштиради[22]. **Германияда** илмий ва суд амалиётида StGB*

*303а-моддасининг маълумотлардан фойдаланиш имкониятини йўқотиш қисми Ransomware шифрлашини тўғридан-тўғри маълумотларни модификация қилиш жинояти сифатида баҳолашга асос бўлади, чунки шифрланган файл ўзининг асл мазмунини йўқотади[23]. **Австралияда** тизимга маълумотлар киритилишига тўсқинлик қилишни (Suppression) тақиқлайди, бу эса тармоқ трафигини блокловчи ёки логин/пароллар тизимини тўхтатиб қўювчи ҳужумларни ўз ичига олади[24]. **Франция** тизимга маълумотларни ноқонуний киритиш ёки ундаги маълумотларни сохталаштиришни тақиқлайди, бу эса сунъий интеллект тизимлари алгоритмларини алдаш учун ишлатиладиган Adversarial Attacks (ғаразли ҳужумлар)ни қамраб олади[25]. **Хитой** компьютер тизимлари функцияларини бузиш, ўчириш ёки ўзгартиришни тақиқлайди, Олий халқ суди шарҳига кўра, маълумотларни устидан янги файл ёзиш (Overwrite) орқали асл нусхани йўқотиш ушбу модда билан жазоланади[26]. **Жанубий Корея** тизимга ишлаш жараёнини секинлаштирувчи ёки маълумотлар форматини бузувчи махсус кодларни (масалан, Ransomware скриптларини) жойлаштиришни қатъиян ман этади[27]. **Исроил** компьютер материалига ноқонуний аралашиш, жумладан унинг кодини ўзгартириш ёки шифрлашни тизим устидан назоратни бузиш сифатида баҳолайди[28]. **Канада** маълумотлардан қонуний фойдаланувчиларнинг улардан фойдаланиш имкониятини йўқотишини (Suppression) мустақил жиноят деб белгилайди[29].* Шу сабабли ушбу модданинг мазкур диспозициясини бугунги кун талабларига мувофиқлаштириш ва жазо муқаррарлигини таъминлаш бугунги кун талабидир;

4) жиноят диспозициясида назарда тутилган “жиддий зиён” тушунчаси амалдаги қонунчиликда назарда тутилган ва бу эса, ушбу модданинг турлича талқин қилинишига олиб келмоқда.

***Маълумот учун**: **АҚШда** жиноий жавобгарлик келиб чиқиши учун ҳужум натижасида етказилган молиявий зарарнинг аниқ минимал миқдори белгиланган – 1 йил давомида камида 5 000 АҚШ доллари миқдорида иқтисодий зиён етказилиши шарт[30]. **Германия** тергов амалиётида "жиддий зарар" тушунчаси ишлатилади ва у корхона фаолиятининг камида бир неча соатга бутунлай тўхтаб қолиши ёки қайта тиклаш харажатларининг сезиларли молиявий қиймати (одатда, 2 500 евродан юқори) билан ўлчанади[31]. **Буюк Британия** зиённи баҳолашда фақат бевосита зарар эмас, балки киберҳужумдан кейин тизимни аудит қилиш ва қайта тиклаш учун жалб этилган ташқи IT-компанияларнинг хизмат ҳақи (Incident Response costs) ҳам жиноий зарар миқдорига қўшиб ҳисобланади[32]. **Малайзия**да зарар тушунчаси тизимни олдинги ҳолатига келтириш учун сарфланган техник соатлар қиймати билан баҳоланади ва у пул эквивалентида суд томонидан ҳисоблаб чиқилади[33]. **БАА** кибержиноятларга оид қисмида давлат реестридаги маълумотларни модификация қилишда моддий зарар миқдоридан қатъи назар, тизимнинг юридик мақоми бузилишининг ўзи автоматик равишда оғир оқибат сифатида баҳоланади[34]. **Саудия Арабистони**да банк ёки молиявий маълумотларни модификация қилишда зарар миқдори муайян пул бирлигига боғланмаган, балки транзакциянинг қонунийлиги бузилган вақтдан бошлаб жиноят тамомланган ҳисобланади[35]. **Сингапур** қонунчиликда зарар (damage) тушунчасига аниқ таъриф берилган бўлиб, у тизимнинг ишлаш қобилияти пасайиши, маълумотларнинг махфийлиги бузилиши ва тизимни қайта созлаш харажатларининг йиғиндисини англатади[36]. **Янги Зеландия** компьютер тизимига ўзгартириш киритиш орқали етказилган зарар БҲМ каби кўрсаткичларга эмас, балки жабрланувчининг кўрган реал зарари (actual loss) ва бой берилган фойдаси (loss of opportunity) асосида*

*судда исботланади[37]. **Ҳиндистонда** маълумотларни модификация қилган шахс жабрланувчига етказилган зарарни компенсация қилиш мажбурияти юкланади, агар зарар 10 миллион рупийдан ошса, у жиноий жавобгарлик мезонига ўтади[38]. **Канада** суд амалиётида компьютер маълумотларини бузишда "жиддий зиён" тизимдан фойдаланувчилар сонига қараб белгиланади: агар ҳужум оммавий давлат хизматлари платформасининг ишини бузган бўлса, моддий зарар кам бўлса ҳам, у ижтимоий хавфи юқори жиноят деб топилади[39];*

5) ЖК 278^4-модданинг жазо қисмидаги асосий муаммо жазо тизимининг қилмишга нисбатан номутаносиблиги, енгиллиги ва нотўғри эканлиги билан характерланади. Айбдор компьютер тизимида сақланаётган ахборотни модификация қилганлиги учун унга озодликни чеклаш ёки ахлоқ тузатиш ишлари жазосининг қўлланилиши айбдорга қўшимча тариқасида жазодан қутилиб қолиш мақсадида бошқа қилмиш содир этиши ёки унга қўйилган чекловларни сунъий равишда четлаб ўтиш ҳолатларига бевосита шарт-шароит яратиб бериши мумкин. Қолаверса, айбдорнинг ҳаракатлари кўп миқдорда зарар, яъни базавий ҳисоблаш миқдорининг уч юз бараваридан беш юз бараваригача бўлган миқдордаги зарар келтириб чиқарган ҳолда, унга базавий ҳисоблаш миқдорининг юз бараваригача миқдорда жарима қўлланилиши ва унинг қуйи чегаралари ҳам белгиланмаганлиги билан айтиш керакки, жазо ва қилмиш ўртасида жиддий номутаносиблик вужудга келган.

***Маълумот учун: Францияда** компьютер тизимидаги маълумотларни ноқонуний модификация қилган шахсларга нисбатан асосий жазодан ташқари, мажбурий равишда **5 йилгача муддатга жиноят содир этишда фойдаланилган касбий ёки ижтимоий фаолият билан шуғулланишни (яъни IT соҳасини) тақиқлаш** қўшимча жазоси қўлланилади[40]. **Германияда** агар кибержиноят шахснинг*

касбий мавқеи (мисол учун, тизим администратори) орқали содир этилган бўлса, суд унга нисбатан камида ***1 йилдан 5 йилгача ёки бутун умрга муайян касбий фаолиятни тақиқлаш (Berufsverbot)*** *тўғрисида ҳукм чиқаради[41].* ***Испания*** *санкциясида тизим ва маълумотларга зарар етказган IT соҳаси ходимларига нисбатан мажбурий равишда* ***муайян касб, ҳунар ёки лавозимни эгаллаш ҳуқуқидан (информатика ва телекоммуникация соҳасида) маҳрум қилиш*** *жазоси кўрсатилган[42].* ***Италия*** *тизим операторларининг киберҳужум содир этиши учун жавобгарликни кучайтириш билан бирга, уларни IT тизимларини бошқариш ҳуқуқидан узоқ муддатга маҳрум этади[43].* ***Польша*** *судларга киберхавфсизлик ва дастурлаш соҳасида ишлаб, тизимдаги маълумотларни сохталаштирган шахсларга нисбатан* ***муайян касб билан шуғулланишни тақиқлаш (zakaz zajmowania określonego stanowiska)*** *қўшимча жазосини бериш мажбуриятини юклайди[44].* ***Япония*** *суд прецедентларига кўра, тизимларни модификация қилган хакерларга нисбатан озодликдан маҳрум қилиш жазоси берилганда, уларнинг қамоқхонада ҳам компьютер ва тармоқ ресурсларидан фойдаланиш ҳуқуқлари махсус режим асосида чекланади[45].* ***Жанубий Корея*** *кибержиноят содир этган шахслар рақамли тизимларга оид давлат шартномалари ва лойиҳаларида (тендерларда) иштирок этувчи компанияларда раҳбарлик лавозимларини эгаллаш ҳуқуқидан қонун йўли билан маҳрум қилинади[46].* ***Бельгия****да судланган шахсларга IT-аудит, тизимларни бошқариш ва провайдерлик компанияларида ишлаш тақиқланади ва бу маҳкумларни назорат қилиш пробация хизмати томонидан амалга оширилади[47].* ***Сингапур*** *такроран кибержиноят содир этган шахсларга нисбатан суд муайян муддатга интернетга уланувчи қурилмаларга эгалик қилиш ва улардан фойдаланишни чеклаш ҳуқуқига эга[48].* ***Швейцария*** *илмий ва суд амалиётига кўра, киберҳужум*

усулида маълумотларни ўзгартирган мутахассисларга нисбатан ***касбий фаолиятни амалга оширишни тақиқлаш (Tätigkeitsverbot)*** *фаол қўлланилади[49].* Бу вазиятда қонунийлик адолатлилик принципидан устун келиши ва кенг жамоатчиликнинг жиддий эътирозларига сабаб бўладиган ҳолатларнинг кўпайишига олиб келиши табиийдир.

6) муҳим ахборот инфратузилмаларига нисбатан киберҳужум содир этилиши оқибатида мазкур қилмиш содир этилган бўлса, ушбу вазиятда айбдорнинг қилмиши билан бошқа инфратузилмаларга нисбатан худди шундай қилмишни содир этган шахсга нисбатан қўлланиладиган жазонинг бир хил қўлланилиши ижтимоий адолат мезонларига ва жамият хавфсизлигини ўз вақтида таъминлаш принципларига тўғри келмайди. Ушбу вазиятда жиноятнинг алоҳида белгиси сифатида муҳим ахборот инфратузилмасига ёки ундаги ахборотга нисбатан содир этилган мазкур ҳаракат учун оғирроқ жазони жиноят қонунчилигимизда акс эттириш даркор.

Маълумот учун: АҚШ *агар маълумотларни модификация қилиш ҳужуми давлат мудофааси, миллий хавфсизлик ёки энергетика тизимлари каби "критик инфратузилма"га қаратилган бўлса, максимал жазо муддати оддий тизимларга нисбатан икки баравар оширилиб, 20 йилгача озодликдан маҳрум қилиш этиб белгиланади[50].* ***Буюк Британияда*** *муҳим инфратузилмага ҳужум қилиш ва маълумотларни ўзгартириш орқали миллий хавфсизликка ёки ҳаётий муҳим хизматларга (сув, свет, тиббиёт) жиддий зарар етказиш учун бутун умрлик озодликдан маҳрум қилиш жазоси назарда тутилган[51].* ***Германияда*** *агар компьютер саботажи жамият учун ҳаётий муҳим аҳамиятга эга бўлган корхоналар ёки давлат органларининг (масалан, АЭСлар, темир йўл тизимлари) маълумотлар базасига зарар етказса, жазо фақат жарима эмас, балки 5 йилгача озодликдан маҳрум қилиш*

*ҳисобланади[52]. **Францияда** давлат аҳамиятига молик тизимлардаги маълумотларни бузишни тақиқлайди, агар ушбу ҳаракат миллий мудофаа манфаатларига дахлдор тизимларга нисбатан содир этилса (323-4-1 модда), жазо 15 йилгача озодликдан маҳрум қилиш ва 300 000 евро жаримага кўтарилади[53]. **Украинада** уруш ҳолати даврида ёки критик инфратузилма объектларига нисбатан маълумотларни ноқонуний модификация қилиш ва тизим ишини бузиш ҳаракатлари учун жавобгарликни кескин кучайтириб, 10 йилдан 15 йилгача озодликдан маҳрум қилиш жазосини белгилайди[54]. **Сингапурда** муҳим ахборот инфратузилмасига (хоҳ давлат, хоҳ хусусий сектор бўлсин) кириш ҳуқуқини суиистеъмол қилиб, маълумотларни ўзгартирганлик учун жазони 20 йилгача озодликдан маҳрум қилиш ва 100 000 доллар жарима қилиб белгилаган[55]. **Исроил** суд ва тергов амалиётида сув таъминоти, ҳарбий тизимлар ёки банк сектори маълумотларига ноқонуний ўзгартириш киритиш ҳаракатлари Давлат хавфсизлиги тўғрисидаги қонун ва "Компьютерлар тўғрисида"ги қонуннинг энг оғир санкциялари остида квалификация қилинади[56]. **Япония**да давлат бошқаруви ва муҳим иқтисодий тармоқларнинг (масалан, Shinkansen тезюрар поездлари тизими) рақамли маълумотларини сохталаштириш ижтимоий хавфи ўта юқори бўлган диверсия сифатида баҳоланади[57]. **Австралия** тизим маълумотларини ўзгартириш орқали иқтисодий ёки инфратузилмавий барқарорликка таҳдид солиш ҳаракатларини оғир кибертеррорчилик усули сифатида баҳолаб, узоқ муддатли қамоқ жазосини назарда тутади[58];*

7) ЖКнинг 278^4-моддасидаги қилмиш ЖКнинг 278^2-моддасида назарда тутилган қилмишга нисбатан оғирроқ эканлиги инобатга олинмаган. Компьютер ахборотини модификациялаштириш ЖКнинг

278[2]-моддасида оқибат нуқтаи назаридан баён этилган бўлса, ЖКнинг 278[4]-моддасида бу қилмиш ҳаракат нуқтаи назаридан баён этилган.

Маълумот учун: Австрияда *тизимли иерархия яратилган: 118а-модда (Тизимга ноқонуний кириш) формал таркибли жиноят бўлиб, агар у маълумотларнинг ўзгаришига олиб келса, у автоматик равишда оғирроқ модда бўлган 126а-модда (Маълумотларни ўзгартириш) билан қамраб олинади ва икки марта квалификация қилинмайди[59].* ***Чехияда*** *компьютер тизими ва маълумотларига ноқонуний киришни ҳамда ундан кейинги маълумотларни ўчириш/ўзгартириш ҳаракатларини ягона модданинг турли қисмлари (иерархик қисмлари) сифатида тартибга солади, бу эса коллизияларни истисно этади[60].* ***Венгрияда*** *ахборот тизимига ноқонуний киришни (1-қисм) ва ушбу кириш орқали маълумотларни модификация қилишни (2-қисм) битта умумий жиноят таркиби сифатида баҳолайди, бу эса жиноятлар мажмуи муаммосини ҳал қилади[61].* ***Словакия*** *жиноят содир этиш усули ва оқибатини ягона нормада бирлаштирган, натижада тергов органлари мажмуавий квалификация қилишга мажбур бўлмайди[62].* ***Румынияда*** *рухсатсиз кириш ва маълумотлар яхлитлигини бузиш ўртасида қатъий субсидиарлик қоидаси амал қилади: агар модификация содир бўлган бўлса, кириш моддаси ўз кучини йўқотади[63].* ***Болгарияда*** *компьютер тизимига киришни ва ундаги маълумотларни модификация қилишни ягона жиноий қасд билан содир этилган қилмиш сифатида кўради[64].* ***Греция*** *кибержиноятларга оид қонунчилик тизимида рухсатсиз кириш кейинги маълумотларни бузиш жиноятининг таркибий қисми (содир этиш усули) сифатида ютиб юборилади ва жазо энг оғир оқибат бўйича берилади[65].* ***Португалияда*** *ноқонуний кириш ва маълумотларни ўзгартириш ўртасидаги нисбатни тартибга солинган ва маълумотлар ўзгартирилган тақдирда, маълумотларни сохталаштириш ёки*

ўзгартириш) қўлланилади[66]. ***Хорватия*** *компьютер тизимининг мазмунини ноқонуний ўзгартиришни мустақил оғир таркиб сифатида белгилайди, тизимга кириш эса ушбу жиноятнинг объектив томони элементларидан бири ҳисобланади[67].* ***Словения*** *ахборот тизимлари хавфсизлигини бузиш умумий номи остида кириш ва модификация ҳаракатларини бирлаштиради ва уларни оқибатига қараб тизимли равишда тақсимлайди[68].* Маълумки, Конституциямизнинг 20-моддасига асосан, инсон билан давлат органларининг ўзаро муносабатларида юзага келадиган қонунчиликдаги барча зиддиятлар ва ноаниқликлар инсон фойдасига талқин этилади[69]. Бу эса, ўз навбатида жиноят учун жазо муқарраплиги принципига зид саналади.

8) ЖКнинг 278^{4}-моддасида назарда тутилган қилмиш хизмат мавқеидан фойдаланиб содир этилганлиги номаълум бўлиб қолганлиги сабабли амалда шу пайтга қадар ушбу қилмиш жиноятлар мажмуи сифатида айбдорнинг ҳаракатлари ЖКнинг 192^{11}-, 205-206-, 301-моддаларида назарда тутилган ҳокимият ёки мансаб ваколатини суиистеъмол қилиш ёки ваколат доирасидан четга чиқиш жиноятлари билан бирга квалификацияланиб келинмоқда ва бу эса, бир қилмиш учун икки хил жазо қўлланилишига сабаб бўлмоқда. Бу ҳолат эса, одиллик принципи талабларига зид саналади.

Маълумот учун: АҚШ *суд амалиётида тизимга қонуний кириш ҳуқуқига эга бўлган ходимнинг (инсайдер) ўз ваколатини суиистеъмол қилиб, маълумотларни модификация қилиши умумий фирибгарлик эмас, балки CFAA қонунининг махсус "exceeding authorized access" (ваколат доирасидан чиқиш) банди билан квалификация қилинишини қатъий белгилаб берган[70].* ***Буюк Британия*** *тизимга кириш ҳуқуқи бор, лекин ундаги маълумотларни ўзгартиришга ҳуқуқи бўлмаган ходимларга нисбатан қўлланилади ва бу умумий хизмат ваколатини суиистеъмол*

*қилиш моддаларини истисно этади[71]. **Сингапур** қонунчилик тизимида ходим томонидан тизим маълумотларини ўзгартириш ҳаракати содир этилса, умумий Коррупция ва суиистеъмоллик тўғрисидаги қонун эмас, балки "Компьютерларни суиистеъмол қилиш тўғрисида"ги қонуннинг "тизим операторлари жавобгарлиги" ҳақидаги махсус бандлари қўлланилади[72]. **Австралия**да давлат ёки тижорат ташкилоти ходими тизимдаги маълумотларни қонунга хилоф равишда таҳрир қилса, унга нисбатан умумий мансабдорлик жинояти эмас, балки кибержиноятнинг оғирлаштирувчи ҳолати қўлланилади[73]. **Канадада** инсайдер томонидан маълумотлар яхлитлигини бузиш ҳаракати компьютер тизимидан ноқонуний фойдаланиш деб топилади ва умумий ишончни суиистеъмол қилиш моддалари билан мажмуа ҳосил қилмайди[77]. **Германияда** тизим администраторлари ёки ходимлар томонидан содир этилса, умумий хизмат жиноятлари (Amtsdelikte) билан эмас, балки ушбу махсус моддаларнинг квалификация қилувчи белгилари билан жазоланади[75]. **Францияда** тизимга кириш ҳуқуқи мавжуд бўлган шахс (инсайдер) томонидан маълумотлар сохталаштирилганда тўғридан-тўғри қўлланилади, бу эса умумий давлат хизматчиси жавобгарлиги нормаларига нисбатан махсус норма (lex specialis derogat legi generali) сифатида устуворликка эга бўлади[76]. **ЖАРда** тизим ва маълумотларни модификация қилишни тақиқлайди, агар ушбу жиноят тизимга қонуний кириш ҳуқуқи бор шахс томонидан содир этилса, жазо сезиларли даражада кучайтирилади[77]. **БААда** банк ходимлари ёки давлат хизматчилари томонидан тизим маълумотларини ўзгартириш ҳаракати умумий мансабдорлик моддаларини четлаб ўтган ҳолда, тўғридан-тўғри махсус кибержиноят сифатида малакаланади[78].* Ўзбекистондаги юқоридаги ҳолат эса, қонун фойдаланувчилари ўртасида қилмишнинг турлича талқин қилинишига ва қонунни қўллаш жараёнида

зиддиятларнинг вужудга келишига сабаб бўлмоқда. Амалиётда, қонун фойдаланувчилари мазкур жиноятнинг умумий қасд билан ўзаро боғлиқлиги жиҳатидан ўзаро фарқ қилишини тушунтириб ўтишади. Бироқ, бу ҳолатнинг қонунда аниқ акс эттирилмаганлиги кенг жамоатчиликнинг асосли эътирозларига сабаб бўлмоқда.

Юқоридагилардан келиб чиқиб, мавжуд муаммони ҳал қилиш учун қуйидагилар таклиф этилади, хусусан, ЖКнинг 278^4-моддасини қуйидаги таҳрирда баён этиш:

“**278^4-модда. Ахборот-коммуникация тизими, тармоғи ва унинг таркибий қисмидаги ахборотнинг яхлитлигига қонунга хилоф тажовуз қилиш**

Ахборот-коммуникация тизими ёки тармоғи ёҳуд унинг таркибий қисмидаги ахборотни қонунга хилоф равишда ўзгартириш, йўқ қилиш, бузиш, сохталаштириш, алмаштириш, шифрлаш, фойдаланиш имкониятини чеклаш ёки бошқа тарзда унинг яхлитлиги, ҳаққонийлиги ёки тўлиқлигига путур етказиш, шунингдек ушбу ахборотга била туриб ёлғон маълумотларни киритиш, агар бу ҳаракатлар фуқароларнинг ҳуқуқларига ёки қонун билан қўриқланадиган манфаатларига ёхуд давлат ёки жамоат манфаатларига кўп миқдорда зарар етказилишига сабаб бўлса,

—

базавий ҳисоблаш миқдорининг юз бараваридан икки юз бараваригача миқдорда жарима ёки уч йилгача муайян ҳуқуқдан маҳрум қилиб, уч йилгача озодликдан маҳрум қилиш билан жазоланади.

Ўша ҳаракатлар:

а) жуда кўп миқдорда зарар етказган ҳолда;

б) бир гуруҳ шахслар томонидан олдиндан тил бириктириб;

в) такроран ёки хавфли рецидивист томонидан;

г) хизмат мавқеидан ёки ахборот-коммуникация тизимига қонуний кириш ҳуқуқидан фойдаланган ҳолда;

д) ғаразли ёки бошқа паст ниятларда;

е) автоматлаштирилган дастурий воситалар, сунъий интеллект технологиялари ёки бошқа техник воситалардан фойдаланган ҳолда содир этилган бўлса, —

уч йилдан беш йилгача озодликдан маҳрум қилиш билан жазоланади.

Ушбу модданинг биринчи ёки иккинчи қисмида назарда тутилган ҳаракатлар:

а) уюшган гуруҳ томонидан ёки унинг манфаатларини кўзлаб;

б) муҳим ахборот инфратузилмаси объектларига, давлат ахборот ресурсларига ёки давлат ахборот тизимларига нисбатан;

в) ўта хавфли рецидивист томонидан содир этилган бўлса;

г) инсон ҳаёти ёки соғлиғига, давлат хавфсизлигига, мудофаа қобилиятига, жамоат хавфсизлигига ёки иқтисодиётнинг муҳим тармоқларига хавф туғдирган ёхуд бошқа оғир оқибатларга сабаб бўлган ҳолда содир этилган бўлса, —

беш йилдан ўн йилгача озодликдан маҳрум қилиш билан жазоланади.

Етказилган моддий зарарнинг ўрни икки ҳисса қопланган тақдирда озодликдан маҳрум қилиш тариқасидаги жазо жарима жазоси билан алмаштирилади.”.

Мазкур қонунчилик комплексининг қабул қилиниши баён этилган 8 та фундаментал муаммони тизимли равишда ҳал этиб, кибермуҳитда, шу жумладан, кибермаконда ҳуқуқни қўллаш амалиётини қуйидаги йўналишларда сифат жиҳатидан янги босқичга олиб чиқади:

1) жиноят қонунчилигидаги “компьютер тизими ва ахбороти” тушунчасининг технологик жиҳатдан бетараф ва кенг кўламли янги таҳрирда баён этилиши миллий рақамли экотизимни концептуал ҳимоя қилишга ҳамда пайдо бўлаётган янги турдаги киберҳужумлар фонида қонунчиликда бўшлиқлар қолишининг олдини олишга;

2) ахборотни модификациялаш, шикастлаш ва ёлғон маълумот киритиш ҳаракатларининг техник чегараларини аниқ ажратиш, шунингдек, “жиддий зиён” мезонига моддий ва функциявий баҳо бериш тизимини жорий этиш ҳуқуқни қўллаш амалиётида (тергов ва судда) қонун нормаларини турлича талқин қилиш ва суиистеъмолчилик имкониятларини бутунлай чеклашга;

3) давлат ахборот ресурслари ва муҳим ахборот инфратузилмаси объектларига қарши қаратилган киберҳужумлар ҳамда замонавий Ransomware (шифрлаш) ва Data Poisoning (маълумотларни заҳарлаш) ҳаракатлари учун махсус оғирлаштирувчи бандларнинг киритилиши миллий хавфсизлик, мудофаа ва иқтисодиётнинг стратегик тармоқлари барқарорлигини кафолатлашга;

4) хизмат мавқеидан фойдаланиб содир этилган кибержиноятларни умумий мансабдорлик моддаларидан ажратиб, махсус норма сифатида квалификация қилиш ҳамда илғор хорижий тажриба асосида айбдорларга нисбатан **“муайян муддатга IT соҳасида ишлаш ва тизимларни бошқариш ҳуқуқидан маҳрум қилиш”** мажбурий қўшимча жазосини жорий этиш кибермаконда жазонинг муқаррарлиги ва профилактика таъсирини сезиларли даражада оширишга хизмат қилади.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР РЎЙХАТИ

1) Ўзбекистон Республикаси Жиноят кодекси // lex.uz – Ўзбекистон Республикаси Қонунчилик маълумотлари миллий базаси.

2) Германия (Strafgesetzbuch) — **gesetze-im-internet.de**

3) АҚШ (Computer Fraud and Abuse Act) — **govinfo.gov**

4) Буюк Британия (Computer Misuse Act 1990) — **legislation.gov.uk**

5) Франция (Code pénal) — **legifrance.gouv.fr**

6) Сингапур (Computer Misuse Act) — **sso.agc.gov.sg**

7) Австралия (Criminal Code Act 1995) — **legislation.gov.au**

8) Канада (Criminal Code) — **laws-lois.justice.gc.ca**

9) Эстония (Karistusseadustik) — **riigiteataja.ee**

10) Жанубий Корея (Ахборот тармоқлари қонуни) — **law.go.kr**

11) Япония (Жиноят кодекси) — **japaneselawtranslation.go.jp**

12) Нидерландия (Wetboek van Strafrecht) — **wetten.overheid.nl**

13) Австрия (Strafgesetzbuch) — **ris.bka.gv.at**

14) Швейцария (Жиноят кодекси) — **fedlex.admin.ch**

15) Италия (Codice penale) — **normattiva.it**

16) Испания (Código Penal) — **boe.es**

17) Польша (Kodeks karny) — **isap.sejm.gov.pl**

18) Дания (Straffeloven) — **retsinformation.dk**

19) Норвегия (Straffeloven) — **lovdata.no**

20) АҚШ (18 U.S.C. § 1030) — **govinfo.gov**

21) Буюк Британия (Computer Misuse Act 1990) — **legislation.gov.uk**

22) Сингапур (Computer Misuse Act) — **sso.agc.gov.sg**

23) Германия (Strafgesetzbuch) — **gesetze-im-internet.de**

24) Австралия (Criminal Code Act 1995) — **legislation.gov.au**

25) Франция (Code pénal) — **legifrance.gouv.fr**

26) Хитой (Жиноят кодекси) — **en.npc.gov.cn**

27) Жанубий Корея (Ахборот хавфсизлиги қонуни) — **elaw.klri.re.kr**

28) Исроил (Computers Law 1995) — **nevo.co.il**

29) Канада (Criminal Code) — **laws-lois.justice.gc.ca**

30) АҚШ (Computer Fraud and Abuse Act) — **govinfo.gov**

31) Германия (Strafgesetzbuch) — **gesetze-im-internet.de**

32) Буюк Британия (Computer Misuse Act 1990) — **legislation.gov.uk**

33) Малайзия (Computer Crimes Act 1997) — **lom.agc.gov.my**

34) БАА (Кибержиноятларга қарши қонун) — **elaws.moj.gov.ae**

35) Саудия Арабистони (Anti-Cybercrime Law) — **laws.boe.gov.sa**

36) Сингапур (Computer Misuse Act) — **sso.agc.gov.sg**

37) Янги Зеландия (Crimes Act 1961) — **legislation.govt.nz**

38) Ҳиндистон (Information Technology Act 2000) — **indiacode.nic.in**

39) Канада (Criminal Code) — **laws-lois.justice.gc.ca**

40) Франция (Code pénal) — **legifrance.gouv.fr**

41) Германия (Strafgesetzbuch) — **gesetze-im-internet.de**

42) Испания (Código Penal) — **boe.es**

43) Италия (Codice penale) — **normattiva.it**

44) Польша (Kodeks karny) — **isap.sejm.gov.pl**

45) Япония (Жиноят кодекси) — **japaneselawtranslation.go.jp**

46) Жанубий Корея (Ахборот хавфсизлиги қонуни) — **law.go.kr**

47) Бельгия (Code pénal) — **ejustice.just.fgov.be**

48) Сингапур (Computer Misuse Act) — **sso.agc.gov.sg**

49) Швейцария (Жиноят кодекси) — **fedlex.admin.ch**

50) АҚШ (Computer Fraud and Abuse Act) — **govinfo.gov**

51) Буюк Британия (Computer Misuse Act 1990) — **legislation.gov.uk**

52) Германия (Strafgesetzbuch) — **gesetze-im-internet.de**

53) Франция (Code pénal) — **legifrance.gouv.fr**

54) Украина (Кримінальний кодекс) — **zakon.rada.gov.ua**

55) Сингапур (Computer Misuse Act) — **sso.agc.gov.sg**

56) Исроил (Computers Law 1995) — **nevo.co.il**

57) Япония (Жиноят кодекси) — **japaneselawtranslation.go.jp**

58) Австралия (Criminal Code Act 1995) — **legislation.gov.au**

59) Австрия (Strafgesetzbuch) — **ris.bka.gv.at**

60) Чехия (Trestní zákoník) — **zakonyprolidi.cz**

61) Венгрия (Büntető Törvénykönyv) — **njt.hu**

62) Словакия (Trestný zákon) — **slov-lex.sk**

63) Руминия (Codul penal) — **legislatie.just.ro**

64) Болгария (Наказателен кодекс) — **lex.bg**

65) Греция (Ποινικός Κώδικας) — **kodiko.gr**

66) Португалия (Lei do Cibercrime) — **dre.pt**

67) Хорватия (Kazneni zakon) — **zakon.hr**

68) Словения (Kazenski zakonik) — **pisrs.si**

69) Ўзбекистон Республикаси Конституцияси // lex.uz – Ўзбекистон Республикаси Қонунчилик маълумотлари миллий базаси.

70) АҚШ (Van Buren v. United States) — **govinfo.gov**

71) Буюк Британия (Computer Misuse Act 1990) — **legislation.gov.uk**

72) Сингапур (Computer Misuse Act) — **sso.agc.gov.sg**

73) Австралия (Criminal Code Act 1995) — **legislation.gov.au**

74) Канада (Criminal Code) — **laws-lois.justice.gc.ca**

75) Германия (Strafgesetzbuch) — **gesetze-im-internet.de**

76) Франция (Code pénal) — **legifrance.gouv.fr**

77) ЖАР (Cybercrimes Act 2020) — **gov.za**

78) БАА (Кибержиноятларга қарши қонун) — **elaws.moj.gov.ae**