Бутунбаев Тимур Нурйигитович
Ўзбекистон Республикаси Жамоат хавфсизлиги университети мустақил изланувчиси

АХБОРОТ ТЕХНОЛОГИЯЛАРИ СОҲАСИДАГИ ЖИНОЯТЛАРГА ҚАРШИ КУРАШДА ХАЛҚАРО ҲУҚУҚИЙ ҲАМКОРЛИКНИНГ ХУСУСИЯТЛАРИ

Бутунбаев Тимур Нурйигитович
Самостоятельный соискатель Университета общественной безопасности Республики Узбекистан

ОСОБЕННОСТИ МЕЖДУНАРОДНО-ПРАВОВОГО СОТРУДНИЧЕСТВА В БОРЬБЕ С ПРЕСТУПЛЕНИЯМИ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Butunbaev Timur
Independent researcher at the University of Public Security of the Republic of Uzbekistan

FEATURES OF INTERNATIONAL LEGAL COOPERATION IN THE FIGHT AGAINST CRIME IN THE FIELD OF INFORMATION TECHNOLOGIES

Аннотация. *Ахборот технологиялари дунёсида киберхавфсизлик муҳим роль ўйнайди. Бугунги кунда ахборотларнинг ҳимояси – ҳукуматлар дуч келадиган муҳим муаммолардан бири. Бу борада эътиборни, биринчи навбатда, нафақат кибержиноятчиликка қарши ишончли ҳуқуқий чораларни амалга оширишга, балки тез ривожланаётган ахборот маконида мазкур кибержиноятларни бартараф этишга йўналтирилган аниқ инструментларни жорий этишга қаратиш лозим. Аммо муаммонинг глобал характерга эгалиги сабабли халқаро ҳуқуқий ҳамкорлик учун мустаҳкам асос яратилмагунга қадар мазкур чораларнинг самарадорлиги шубҳали туюлади. Шундай қилиб, мазкур мақолада халқаро кибержиноятчиликка қарши қаратилган қонунчилик ва конвенцияларни қабул қилаётган ҳукуматлар дуч келаётган муҳим муаммолар, шунингдек, мазкур соҳада халқаро ҳамкорлик учун глобал асос яратишнинг потенциал истиқболлари муҳокама қилинмоқда.*

Таянч иборалар: *халқаро киберхавфсизлик, кибержиноятчилик, ахборот макони, жиноятчиликка қарши курашиш, халқаро ҳамкорлик*

Аннотация. *В мире информационных технологий кибербезопасность играет важную роль. Защита данных – одна из самых серьезных проблем, с которыми сегодня сталкиваются правительства. В этом случае первое, что необходимо принять во внимание – это не только реализация надежных правовых мер по борьбе с киберпреступностью, но и внедрение конкретных инструментов, которые могут существенно предотвратить эти киберпреступления в быстрорастущем информационном пространстве. Однако эффективность этих мер представляется сомнительной с учетом глобального характера проблемы, если не будет создана прочная основа для международного правового сотрудничества. Таким образом, в данной статье рассматриваются существующие проблемы, с которыми сталкиваются правительства, принимающие законодательство и конвенции против киберпреступности, а также обсуждаются потенциальные перспективы единой глобальной основы для международного сотрудничества в этой области.*

Ключевые слова: *международная кибербезопасность, киберпреступность, информационное пространство, борьба с преступностью, международное сотрудничество.*

Abstract: *Cybersecurity plays an important role in the world of information technology. Securing data is one of the biggest challenges that the governments are facing today. In this case, the first thing that has to be taken into consideration is not only the implementation of solid legal measures to fight cybercrime, but also introducing specific tools that can essentially prevent those cybercrimes on rapidly growing information space. However, the effectiveness of these measures seem questionable given the global nature of the problem, unless a solid foundation for international legal cooperation is established. Thus this article looks at the existing challenges faced by governments that are adopting international legislations and conventions against cybercrime and also discuss the potential prospects of a single global framework for international cooperation in this area.*

Keywords: *international cybersecurity, cybercrime, information space fighting crime, international cooperation*

Жаҳон ҳамжамияти кибержиноятчиликка қарши курашиш, кибертизимларнинг барқарорлигини ошириш ва ахборот хавфсизлигини таъминлашнинг бошқа жиҳатларига катта эътибор қаратмоқда. Турли мамлакатлар томонидан амалга оширилаётган чора-тадбирлар кибержиноятчилик муаммосининг глобал моҳиятини тушунишга имкон бермоқда. Шундай экан, энди киберҳужумлар нафақат хусусий тузилмалар, балки давлат органларининг ишини тўхтатмоқда, дунёда бундай ҳужумлардан ҳимояланган давлат мавжуд эмас.

Киберхавфсизлик бўйича етакчи тадқиқотчи Cybersecurity Ventures маълумотларига кўра, “2021 йилга келиб, кибержиноятчилик дунёга йилига 6 триллион доллар зарар етказди, яъни бу табиий офатлар оқибатида етказилган зарардан кўпроқ ва дунё бўйлаб ҳар қандай ноқонуний гиёҳванд моддаларни сотишдан кўра даромадлироқдир” [1].

Дарҳақиқат, замонавий дунёда ҳаётнинг барча соҳалари ҳисоблаш ва ахборот тармоқларининг ишлашига бевосита боғлиқдир. Шу билан бирга, “ахборотни қайта ишлаш учун компьютер технологияларидан кенг фойдаланилиши дастурий таъминот ёрдамида маълумотни ўзгартириш, нусхалаш ва йўқ қилишни нисбатан осонлаштириши” [2] ахборот маконининг заифлигини оширади. Ахборот тизимларининг фойдаланувчилари “ахборот маконидаги чекловлар ва тизим хавфсизлигига бўлган таҳдидлар борасида билмасдан фойдаланган ҳолда киберҳужумлар мавжуд эмаслигига маълум бир сабабларсиз ишонишади” [3].

Масалан, жаҳон экспертлари, оммавий ахборот воситалари ва сиёсий мунозараларда “Covid-19” коронавирус инфекцияси тўғрисида интернет орқали сохта маълумотларнинг тарқалиши аҳоли орасидаги ваҳимада ҳал қилувчи роль ўйнади, бу бир қатор товарларга бўлган талабни кучли даражада ўзгартирди.

Ҳозирги вақтда ахборот энг муҳим неъматлардан бири сифатида эътироф этилади, мос равишда, уни ҳимоя қилиш уни қабул қилиш ва узатишдан ҳам кўра муҳим аҳамиятга эгадир, “XXI аср бошидаги рақамли жамиятда хавф даражасининг намоён бўлиши ўзгариб бормоқда” [4].

Кибержиноятчилик соҳасидаги қонун ҳужжатларини уйғунлаштириш бўйича халқаро эксперт Штайн Шйолберг (Stein Schjolberg) таъкидлаганидек, “Кибермакон қуруқлик, денгиз, ҳаво ва космосдан кейин турувчи бешинчи умумий макон сифатида халқаро миқёсда мувофиқлаштириш, ҳамкорлик ва махсус ҳуқуқий чора-тадбирларни талаб қилади” [5].

Кибержиноятчиликка “кибермаконда” жиноят деб қаралади. Кибермакон ёки виртуал маконга компьютер ёрдамида шакллантириладиган ахборот макони сифатида қараш мумкин бўлиб, маҳаллий ва глобал компьютер тармоқларида ҳаракатда бўлган ҳамда математик, рамзий ёки бошқа ҳар қандай кўринишда тақдим этиладиган шахслар, жисмлар, фактлар, воқеа-ҳодисалар ва жараёнлар тўғрисидаги маълумотлар ёки ҳар қандай моддий ёки виртуал қурилма, шунингдек, уларни сақлаш, қайта ишлаш ва узатиш учун махсус ишлаб чиқилган бошқа ташувчилар хотирасида сақланадиган маълумотлардир [6].

Кибержиноятчиликка қарши курашиш бўйича восита ва усулларни ишлаб чиқишда ушбу турдаги жиноятчиликнинг яширинлигини ёдда тутиш лозим. Мутахассисларнинг баҳолашларига кўра, АҚШда “компьютер жиноятларининг” яширинлик даражаси 80 фоиз, Буюк Британияда – 85 фоиз, Германияда – 75 фоиз, Россияда – 90 фоиздир [7].

Ахборот тизимларининг ишлаш хусусиятлари “киберхавфсизлик билан боғлиқ муаммоларни ҳал қилишда турли субъектлар, яъни давлат ва хусусий шахсларнинг биргаликдаги саъй-ҳаракатларини талаб қилади” [8], аммо фақат давлатгина кибержиноятчиликка қарши кенг кўламли курашни самарали амалга оширишга қодир бўлиб, мазкур йўналишда хавфга учраши мумкин бўлганлар учун ахборотни ҳимоя қилишнинг ишончли тизимларини яратиб бера олади.

Дунёда кибержиноятларга қарши кураш бўйича самарали тизимларнинг мисоллари мавжуд. Ҳозирги вақтда дунёнинг етакчи мамлакатлари қуролли кучлар ва махсус хизматлар таркибида кибермаконда ҳужум қилиш қобилиятини ривожлантиришни таъминлайдиган бўлинмаларни фаол равишда яратмоқда ва кенгайтирмоқда (жадвал) [9].

Бир қатор мамлакатларда киберхавфсизликни таъминлаш хусусиятлари

Давлат	Кибержиноятчилик бўйича конвенцияда иштирок этиш	"Халқаро ахборот хавфсизлигини таъминлаш тўғрисида" БМТ Конвенциясини ишлаб чиқиш	Киберхавфсизликни таъминлаш соҳасида фаолият олиб борувчи асосий ташкилотлар
Буюк-Британия	+	–	Ташқи ишлар вазирлиги қошида Ҳуқуқий алоқа маркази электрон коммуникация хавфсизлиги гуруҳи; виртуал таҳдидлардан ҳимоялаш бўйича Мудофаа вазирлиги бўлинмаси
Германия	+	–	ГФР ИИВ қошида махсус гуруҳ
Ҳиндистон	+	–	Ташқи разведка таҳлил ва тадқиқот бўлими ва ички разведка қидирув бўлими
Хитой	–	+	Комьпютерга рухсатсиз уланишдан ҳимоя қилиш дастурини амалга ошириш
Россия	–	+	ИИВ "К" бошқармаси ва ИИВ ҳудудий бошқармаларининг "К" бўлимлари; Россия ИИВ БСТМ қошида миллий алоқа пункти
АҚШ	+	–	Киберхавфсизлик миллий маркази; АҚШ қуролли кучлари кибернетика қўмондонлиги

Масалан, АҚШда фаолият юритаётган Миллий Киберхавфсизлик Маркази (National Cyber Security Center) билан бир қаторда, Қуролли Кучлар таркибида Бирлашган кибернетика қўмондонлиги (Unified U.S. Cyber

Command) ташкил этилган, у глобал миқёсда Пентагоннинг барча тузилмаларини ҳарбий ҳаракатлар пайтида мувофиқлаштириб туриши, фуқаролик федерал институтларини қўллаб-қувватлаш, шунингдек, бошқа мамлакатларнинг ўхшаш идоралари билан ўзаро ҳамкорликда ишлаши лозим [10]. Бироқ мазкур ташкилотлар қисман назорат қилинадиган идоралардир, чунки "энг юқори назорат қилувчи тузилма – бу махсус қўмиталарга эга Миллий хавфсизлик кенгаши бўлиб, унинг вазифаси ахборот стратегиясини амалга ошириш", шу жумладан, кибержиноятчиликка қарши курашишдир.

Буюк Британияда кибермаконда ўсиб бораётган таҳдидларга ҳокимиятнинг қарши тура олиш қобилиятини таъминловчи киберқурол дастурларини яратиш амалга оширилмоқда [11].

Австралияда электрон почта хавфсизлигини мувофиқлаштирувчи гуруҳ (ESCG) яратилган бўлиб, "ушбу гуруҳнинг асосий вазифаси жамият ва хусусий сектор учун хавфсиз ва ишончли, тезкор электрон маконни яратишдир" [12].

Кибержиноятларнинг содир этилишига қарши курашиш нафақат алоҳида давлатлар, балки уларнинг блоклари, хусусан, НАТО томонидан ҳам амалга оширилади. Шундай экан, ушбу муаммонинг аҳамияти блокнинг сўнгги йилларда қабул қилинган барча бошқарув ҳужжатларида акс эттирилган. НАТОнинг стратегик концепциясига илк маротаба иттифоқ ҳарбий фаолиятининг янги йўналиши сифатида кибермакон тўғрисидаги низом киритилган [13].

Таҳлиллар шуни кўрсатадики, трансчегаравий жиноятлар, шу жумладан, кибержиноятларга қарши курашда давлатлар алоҳида аҳамият касб этади ва фақат турли мамлакатлар ҳуқуқни муҳофаза қилиш органларининг яхши мувофиқлаштирилган ишлаши орқали ушбу соҳада содир этиладиган жиноятлар сонининг кескин камайишига эришиш мумкин.

Халқаро ҳамкорлик бир неча йўналишларда амалга оширилади ва, биринчи навбатда, меъёрий ҳужжатларни яратишни ва умумий тавсияларни ишлаб чиқишни, шунингдек, давлатлар ўртасидаги ташкилий ҳамкорликнинг самарали моделларини жорий қилишни ўз ичига олади.

Шуни инобатга олиш лозимки, халқаро ҳамкорликнинг анъанавий механизмлари, яъни сўровлар, ўзаро ёрдам ва бошқа шу каби XIX асрда ва ундан олдин қўллаб келинган воситалар, жиноятларнинг ер шарининг исталган нуқтасидан туриб ёруғлик тезлигида амалга оширса бўладиган даврда ноўрин бўлиб ҳисобланади [14].

Кибержиноятларга қарши курашиш масалаларининг ҳуқуқий тартибга солиниши – бутун кибержиноятчиликка қарши курашиш тизимининг асосидир. Умуман олганда, мазкур вазиятда "далиллари тарқоқ ва виртуал бўлган бутунжаҳон миқёсдаги маҳаллийлаштириб бўлмайдиган хуружлар тўғрисида гап кетганда, мавжуд қонунларни қўллаш қийин" [15]лиги халқаро актларни ишлаб чиқишни янада мураккаблаштиради.

Халқаро ҳамжамият турли даражада кибержиноятчиликка қарши курашиш учун долзарб бўлган бир қатор актларни ишлаб чиққан, бунда бугунги кунда умумжаҳон актни яратиш қийинлиги сабабли минтақавий актлар алоҳида роль ўйнамоқда. Шу билан бирга, давлатларнинг глобал халқаро актлар нормаларини кибержиноятчиликка қарши курашишга йўналтириши ёки янги шартномалар тузиш ҳаракатларини айтиб ўтиш жоиз. Мисол учун, кибермаконда алоҳида шахслар қаторида уюшган жиноий гуруҳлар ҳам фаолият юритиши мумкинлиги, уларга нисбатан уюшган жиноятчиликка қарши курашишга қаратилган халқаро шартномаларни ишлатиш имкони мавжуд, хусусан, БМТнинг 2000 йил 15 ноябрдаги Трансмиллий уюшган жиноятчиликка қарши Конвенцияси.

Бундан ташқари, халқаро ахборот хавфсизлигини таъминлаш тўғрисидаги БМТ Конвенциясининг концепцияси ишлаб чиқилган бўлиб [16], у халқаро ҳамжамиятга 2011 йил ноябр ойида Лондонда кибермаконда ўтказилган конференцияда тақдим этилган бўлиб, преамбула асосий қисмга бирлаштирилган 23 та модда ва якуний қоидаларни ўз ичига олган. Ҳужжатнинг асосий қисми бешта бобдан иборат бўлиб, уларнинг таркиби яхлитдир. Шуни таъкидлаш жоизки, Конвенциянинг 4-бобида халқаро тинчлик ва хавфсизликка таҳдид солувчи хавфлар ёритиб берилиб, уларда 11 та асосий ва 4 та қўшимча таҳдидлар қайд этилган. Уларнинг асосийлари орасида, масалан, ёвуз ва тажовузкор ҳаракатларини амалга оширишда ахборот технологиялари ва воситаларидан фойдаланиш; ахборот маконида бошқа давлатнинг муҳим тузилмаларига мақсадли вайронкор таъсир; халқаро ҳуқуқ принциплари ва нормаларига, шунингдек, давлатлар миллий қонунларига зид келадиган ахборотни трансчегаравий равишда тарқатиш кабилар келтирилган. Шунга қарамай, ҳужжатда кибержиноятлар, гиёҳвандлик воситалари ва психотроп, ёки уларга ўхшаш, дориларни тарқатиш, шунингдек, порнография, шу жумладан, болалар порнографияси каби халқаро хавфсизликка таҳдидлар кўрсатилмаган.

Бундан ташқари, Конвенция концепциясида 5-модда халқаро ахборот хавфсизлигини таъминлашнинг асосий тамойилларига бағишланган. Тақдим этилган принципларнинг таҳлили уларни тўрт гуруҳга бўлиш мумкин, деган хулосага келишга имкон беради: халқаро ахборот хавфсизлиги тизимида давлатнинг халқаро ҳамжамият аъзоси сифатида иштирок этиш тамойиллари; кибержиноятчиликка қарши курашнинг халқаро ҳамкорлик жараёнида давлатга суверенитетини сақлаб қолиш имконини берадиган принциплар; давлатлар ўртасида бепул ахборот алмашинувини таъминлаш тамойиллари. Принципларнинг тўртинчи гуруҳи кўриб чиқилаётган муносабатларда давлат ва хусусий шахсларнинг ўзаро таъсирини белгилайди. Шу билан бирга, Конвенция концепциясида кибержиноятларга қарши курашда халқаро ҳамкорлик тамойиллари тўлиқ баён этилмаганлигини яна бир бор айтиш жоиз, террорчилик актларига қарши қаратилган тамойиллар бундан мустасно.

Конвенция концепциясига “Халқаро ахборот хавфсизлиги соҳасидаги халқаро ҳамкорлик” бешинчи бобининг киритилишини ижобий деб ҳисобланишига қарамай, бу соҳадаги халқаро ҳамкорлик чоралари халқаро иқтисодий хавфсизлик тизимининг самарали ишлаши учун етарли эмас, чунки улар фақат “ахборот маконида хавфсизликни таъминлаш учун миллий концепциялар алмашинуви, ахборот маконида инқироз ҳолатлари ва таҳдидлари тўғрисида тезкор маълумот алмашинуви ва уларни тартибга солиш ва бартараф этиш бўйича чора-тадбирлари”, “иштирокчи давлатларни ташвишга солувчи ва ҳарбий характерга эга низоли вазиятларни тартибга солиш каби муносабатлардаги ҳамкорлик масалаларида ахборот маконидаги ҳаракатлар бўйича маслаҳатлар” ни назарда тутади. Шунга қарамай, ушбу шакллар кенг кўламли масалалар бўйича ҳуқуқни муҳофаза қилиш органларининг ўзаро тезкор ҳамкорлиги зарурлигини назарда тутмайди.

Шу орқали халқаро ахборот хавфсизлигини таъминлаш бўйича БМТ Конвенциясининг концепциялари моҳиятига кўра муросага эга ва, асосан, ахборот урушлари ва терроризмнинг олдини олишга қаратилган.

Таъкидлаш керакки, кибержиноятларга қарши курашга ихтисослашган аксарият актлар дунёдаги энг ривожланган ахборот хавфсизлиги тизимларидан бирига эга Европа Иттифоқининг актлари ҳисобланади. Шундай қилиб, 1999 йил октябрь ойида Европа Кенгашининг Тампере шаҳрида бўлиб ўтган йиғилишида кенгаш томонидан юқори технологиялар соҳасидаги жиноятларни криминал ва санкциялар нуқтаи назаридан умумий Европа ёндашувини ишлаб чиқиш зарур бўлган жиноятлар сонига қўшишни мақсадга мувофиқлиги тўғрисида қарор қабул қилинд [17].

2001 йилда Европа Комиссияси “Ахборот инфратузилмаси хавфсизлигини ошириш ва компьютер воситаларидан фойдаланган ҳолда жиноятчиликка қарши курашиш орқали хавфсиз ахборот жамиятини яратиш” [18] номли махсус хабарни тақдим этди, унда Европа Иттифоқида кибержиноятларга қарши кураш бўйича ҳуқуқий ва ташкилий таклифлар мавжуд.

Европа Иттифоқи учун ҳам, бутун дунё ҳамжамияти учун ҳам 2001 йилда Европа Кенгаши томонидан қабул қилинган кибержиноятларга нисбатан глобал муносабатни тартибга солувчи кибержиноятлар тўғрисидаги Конвенция [19] муҳим аҳамиятга эга ҳисобланади.

Конвенциянинг кириш қисмида иштирокчи давлатлар уни қабул қилишнинг мақсад-моҳиятини белгилаб қўйдилар: устувор вазифа сифатида жиноий қонунчилик соҳасида жамиятни кибержиноятдан ҳимоя қилишга, шу жумладан, тегишли қонунларни қабул қилиш ва халқаро ҳамкорликни кучайтиришга қаратилган ягона сиёсатни ишлаб чиқиш белгиланди: компьютер тизимлари ва тармоқларидан фойдаланишнинг суиистеъмол қилинишини олдини олиш, шунингдек, компьютер

маълумотларининг махфийлиги, яхлитлиги ва улардан фойдаланилишига қарши ҳаракатларни чеклаш, бундай хатти-ҳаракатларнинг жиноий жазосини таъминлаш ва ушбу жиноий ҳуқуқбузарликларга қарши самарали курашиш учун етарли ваколатлар бериш орқали бундай жиноий ҳуқуқбузарликларни аниқлаш ва тергов қилиш ҳамда уларни ички ва халқаро миқёсда ҳамда тезкор ва ишончли халқаро ҳамкорлик тўғрисида битимлар ишлаб чиқиш орқали жавобгарликка тортиш.

Кибержиноятларга қарши кураш тўғрисидаги Конвенция иштирокчи давлатлар даражасида ва халқаро даражада ҳаракатларни амалга оширишни кўзда тутади. Миллий миқёсда, биринчи навбатда, жиноий қонунчиликни ишлаб чиқиш кўзда тутилмоқда: компьютер тизимлари, тармоқлари ва маълумотларнинг махфийлиги, яхлитлиги ва очиқ фойдаланишга қарши жиноятлар, компьютер воситаларидан фойдаланиш билан боғлиқ жиноятлар, маълумотлар таркиби, муаллифлик ҳуқуқи ва турдош ҳуқуқларнинг бузилиши; жавобгарлик ва санкцияларнинг қўшимча турларини белгилаш (жиноят содир этишга уринганлик, ушбу жиноят таркибига кирганлик ёки кўриб чиқилаётган соҳада уни содир этишга ундаш каби жиноятлар таркибига киритиш); юридик шахсларга нисбатан жиноий жавобгарликни белгилаш, бироқ бу бир қатор мамлакатларда, масалан, Ўзбекистон Республикасида жиноий жавобгарлик тушунчаларига зид келади.

Шу тариқа Кибержиноятлар тўғрисидаги Конвенцияда кибержиноятлар қуйидагича таснифланади:

1) компьютер маълумотлари ва тизимларининг махфийлиги, яхлитлиги ва фойдаланиш ҳуқуқига қарши жиноятлар (offences against the confidentiality, integrity and availability of computer data and systems): ноқонуний кириш (illegal access); ноқонуний ушлаб қолиш (illegal interception); маълумотларга таъсир қилиш (data interference); тизимнинг ишлашига таъсир қилиш (system interference); қурилмалардан ноқонуний фойдаланиш (misuse of devices);

2) компьютер воситаларидан фойдаланиш билан боғлиқ ҳуқуқбузарликлар (computer-related offences): компьютер технологияларидан фойдаланган ҳолда қалбакилаштириш (computerrelated forgery); компьютер технологияларидан фойдаланган ҳолда фирибгарлик уюштириш (computerrelated fraud);

3) маълумотлар таркибига оид ҳуқуқбузарликлар (content-related offences) – болалар порнографияси билан боғлиқ ҳуқуқбузарликлар (offences related to child pornography);

4) муаллифлик ҳуқуқи ва турдош ҳуқуқларнинг бузилиши билан боғлиқ ҳуқуқбузарликлар (offences related to infringements of copyright and related rights).

Кибержиноятлар тўғрисидаги Конвенцияга қўшимча протокол[20] юқоридаги рўйхатдаги жиноятларнинг қуйидаги турларини ўз ичига олади:

1) ирқчилик ва ксенофобик материалларни компьютер тизимлари орқали тарқатиш (dissemination of racist and xenophobic material through computer systems);

2) ирқчилик ва ксенофобияга асосланган таҳдид (racist and xenophobic motivated threat);

3) ирқчилик ва ксенофобик асосли ҳақорат (racist and xenophobic motivated insult);

4) геноцид ёки инсониятга қарши жиноятларнинг рад этилиши, ҳаддан ташқари минималлаштирилиши, қўллаб-қувватланиши ёки оқланиши (denial, gross minimization, approval or justification of genocide or crimes against humanity).

Конвенция, шунингдек, жиноий процессуал қонунчиликни ишлаб чиқишни, масалан, тўпланган компьютер маълумотларининг операцион хавфсизлигини, сақланган компьютер маълумотларини қидириш ва мусодара қилишни қонуний жиҳатдан мустаҳкамлаш зарурлигини назарда тутади.

Конвенцияда халқаро ҳамкорликка алоҳида эътибор берилиб, ушбу масала 3-бобда ёритилган. Халқаро ҳамкорликнинг умумий принциплари сифатида қуйидагилар келтирилган: ўзаро ёрдамнинг умумий тамойиллари; тегишли розилик орқали сақланадиган компьютер маълумотларига трансчегаравий кириш имконияти, сақланган электрон маълумотларни баҳолаш муносабати билан ўзаро ёрдам, оқимлар бўйича реал вақт режимида маълумотларни тўплашда ўзаро ҳуқуқий ёрдам; 24/7 тармоғини яратиш.

Ушбу соҳада бошқа халқаро ҳужжатлар мавжудлигига қарамай, “Конвенция тан олинган ягона халқаро шартнома... кибержиноятларга қарши курашиш ва интернетда эркинлик, хавфсизлик ва инсон ҳуқуқларини ҳимоя қилиш учун амалий ва процессуал қонунларни ўз ичига олади” [21].

Конвенция қоидалари давлатлар ўртасидаги ўзаро муносабатлар учун замин яратади, аммо болгар тадқиқотчиси Р. Георгиева таъкидлаганидек: “Конвенция виртуал макон хавфсизлигини кафолатламайди. Уни ҳар бир мамлакатнинг ички қонунлари билан мувофиқлаштириш катта аҳамиятга эга” [22].

Европа Иттифоқи доирасида кибержиноятларга қарши курашга ёрдам берадиган қатор дастурлар амалга оширилмоқда ва бу борада қўшма позициялар ишлаб чиқилмоқда. Хусусан, Стокголм дастури фуқаролар ҳимоясини яхшилаш, уюшган жиноятчилик ва терроризмга қарши курашиш мақсадида ЕИ учун ички хавфсизлик стратегиясини тайёрлашни тавсия қилади.

Минтақавий даражада Кибержиноятларга қарши кураш тўғрисидаги Конвенцияга қўшимча равишда 2001 йил 1 июнда Мустақил Давлатлар Ҳамдўстлигига аъзо давлатларнинг компьютер ахборот жиноятларига қарши курашда ўзаро ҳамкорлиги тўғрисида битими қабул қилинди. Ушбу ҳужжатларнинг асосий ғояси "давлатлар ўз миллий қонунчилигига киритиши керак бўлган компьютер жиноятларининг бир хиллигини аниқлашдан, шунингдек, уларга қарши кураш чораларини ишлаб чиқишдан иборатдир.

Кўриб чиқилаётган шартномалар жуда муҳим аҳамият касб этади: улар интернетдаги жиноий ишлар бўйича давлатлар юрисдикциясининг асосларини ва давлатлараро ҳамкорлик қоидаларини ўрнатиб, компьютер жиноятчилигига қарши курашишдаги давлатлар ҳаракатларининг уйғунлигини таъминламоқда. Шартномадаги айрим камчиликларга қарамай, умуман олганда, улар компьютер жиноятларига қарши курашда ўзаро боғлиқ халқаро ва миллий чоралар тизимини таъминлаб келмоқда" [23].

Шуни таъкидлаш жоизки, кибержиноятчиликка қарши курашда ва унга қарши турли воситалардан фойдаланиш жараёнида давлатлараро ҳамкорлик турли давлатларнинг ҳуқуқий нормаларини умумлаштиришни талаб қилади. Хусусан, НАТО Компьютер хавфсизлигини ошириш маркази томонидан "Киберурушда халқаро ҳуқуқни қўллаш бўйича Таллин кўрсатмалари" номли тавсиялар тўплами нашр этилди. Асосий вазифалар қуролли можароларга нисбатан мавжуд ҳуқуқий нормаларни виртуал маконда душманлик ҳаракатларининг хусусиятларига мослаштириш ва компьютер хавфсизлиги соҳасидаги асосий тушунчаларнинг таърифларини ишлаб чиқишдир.

Кибержиноятларга қарши курашда давлатлар ўртасидаги ҳамкорликнинг иккинчи шакли ихтисослашган идораларни яратишдир.

Давлатнинг ахборот хавфсизлиги унинг суверенитети билан боғлиқ бўлганлиги сабабли кибержиноятчиликка қарши курашишда давлатларнинг ўзаро муносабатларини мувофиқлаштирадиган ягона органни яратиш қийин, аммо ёрдамчи органлар турли мамлакатларнинг кибержиноятларга қарши курашиш амалиётига ва улар фаолиятининг умумий стандартларига асосланиб яратилмоқда.

Европа Иттифоқига аъзо давлатлар ҳамкорлигида "Европа Иттифоқида кибержиноятчиликка қарши курашда бевосита иштирок этувчи" [24] Европол ва Евроюст фаолияти муҳим аҳамиятга эга. Европол фаолиятида ишчи картотекалар таҳлилий тизимидан (Analys Work files) фойдаланилиб, улар тизим таркибидаги файллардан ташкил топган ва жиноий терговни қўллаб-қувватлашда ушбу маълумотлар таҳлилий равишда қайта ишланади. Мавжуд картотекали таҳлил тизимига Cyborg каби кибержиноятчиликка доир картотека ва Twins болалар порнографияси картотекалари киради [25].

Евроюстга келсак, унинг Европада хавфсизликни таъминлаш борасидаги фаолияти тобора равшан бўлиб бормоқда: агар 2015 йилда у 2 311 та ишни тергов қилган бўлса, 2018 йилда 3 317 та ҳолат қайд

этилган [26]. Евроюст, шу қаторда, турли давлатлардаги ҳуқуқни муҳофаза қилиш органларининг кибержиноятни текшириш бўйича ҳаракатларини мувофиқлаштиради, Европа Иттифоқига аъзо давлатларнинг тегишли давлат органлари илтимосига биноан терговларни ўтказишда ёрдам беради ва ушбу давлатларнинг ҳуқуқни муҳофаза қилиш органларига кибержиноятлар бўйича олиб борилаётган тергов ишлари тўғрисида маълумот беради.

Евроюст ваколатлари, шунингдек, жиноий терговларни қўзғатиш ёки уларни қўзғатиш бўйича таклифларни Европа Иттифоқига аъзо давлатларнинг ҳуқуқни муҳофаза қилиш органларига юбориш ва давом этаётган терговларни мувофиқлаштиришга ҳам тааллуқлидир.

Ушбу соҳада юрисдикцияга эга бўлган юқорида таъкидланган органларга қўшимча равишда Европа Иттифоқи томонидан ёрдамчи ташкилотлар ҳам яратилмоқда. Шу тарзда 2013 йил 18 январда Гаагада Европа Кибержиноятларга қарши кураш маркази расман очилди. Унинг яратилишининг сабаблари кибержиноятлар тўғрисидаги маълумотларни тўплаш ва қайта ишлаш, интернет таҳдидларига нисбатан эксперт баҳолашини ўтказиш, кибержиноятларнинг олдини олиш ва тергов қилишнинг илғор усулларини ишлаб чиқиш ва жорий этиш, янги кадрлар тайёрлаш, ҳуқуқни муҳофаза қилиш ва суд органларига ёрдам бериш, шунингдек, манфаатдор томонларнинг қўшма ҳаракатларини мувофиқлаштириш ҳамда Европа кибермаконида хавфсизлик даражасини ошириш [27].

Давлатларнинг ҳарбий ҳамкорлиги кибержиноятларга қарши курашни ташкилий жиҳатдан қўллаб-қувватлаш соҳасидаги ҳамкорлик масаласини ҳам ҳал қилишни талаб қилади. Шундай қилиб, 2008 йилда “Эстониянинг ташаббуси билан Таллинда НАТОнинг илғор тажриба маркази ташкил этилди, ҳозирда бу идора – кибермакондаги ҳаракатларда коалиция имкониятларини ривожлантириш учун муҳим йўналишларни ишлаб чиқаётган илмий-тадқиқот ва таълим муассасасидир” [28].

Ушбу марказнинг ташкил этилиши Шимолий Атлантика кенгашида кибержиноятларга қарши курашни ташкил этишнинг ягона йўналиши эмас эди: 2013 йилда кибермакон таҳдидларига жавоб қайтаришга йўналтирилган иккита марказни (Брюссел ва Монс шаҳарларида) ўз ичига олувчи компьютер таҳдидларига жавоб қайтариш учун НАТОнинг ягона тизимини ишга тушириш ниҳоясига етказилди. Бундан ташқари, киберҳужумларни қайтариш учун аллақачон яратилган тизимнинг самарадорлигини синаб кўриш бўйича чоралар кўрилмоқда, масалан, ҳар йили “Киберкоалиция” ва “Мудофаа тўпи” машқлари ўтказилади.

Бошқача қилиб айтганда, кибержиноятчиликка қарши халқаро муносабатларда ҳозирги тенденция давлатлар ўртасидаги ўзаро таъсир доирасини кенгайтиришдир. Ҳуқуқни муҳофаза қилиш органларининг кибержиноятларга қарши кураш бўйича тезкор ҳамкорлиги (Интерпол,

Европол, Евроюст), кибержиноятчилар, содир этилган ва режалаштирилган кибержиноятлар бўйича ягона маълумотлар базасини яратиш ва улардан фойдаланиш замон талабига айланмоқда.

Баъзи олимларнинг таъкидлашича, Интерполнинг маълумотларга ишлов бериш тезлиги унчалик катта бўлмаган ихтисослашган ташкилотларга қараганда анча самарасиз. Шу сабабли Россия ҳуқуқ-тартибот идоралари 24/7 форматида ишлайдиган ҳамда яқин ва узоқ хориждаги ҳамкасблар билан ўзаро алоқаларни таъминлаш учун ишлаб чиқилган Россия Ички ишлар вазирлигининг Махсус техник тадбирлар бюроси қошидаги Миллий алоқа марказининг имкониятларидан кўпроқ фойдаланадилар. Бир мамлакат махсус бўлинмаси ходими куннинг исталган вақтида бошқа давлатда жойлашган худди шундай пункт билан тезда боғланиб, тезкор-қидирув тадбирларини ўтказиш учун зарур бўлган маълумотларни олиши ёки юбориши мумкин. Бугунги кунда 50 га яқин мамлакатда миллий алоқа пунктлари фаолият кўрсатмоқда [29].

Хулоса қилиб айтганда, кибержиноятларнинг мураккаблиги ва хавфлилигини ҳисобга олиб, ҳуқуқшунос олимлар, қонун чиқарувчи, ахборот технологиялари мутахассисларининг глобал ахборот тармоқларида жиноятчиликка қарши курашишга қаратилган бирлашган ҳаракатларини ишлаб чиқиш зарур. Норматив-ҳуқуқий ҳужжатларнинг ҳам миллий, ҳам халқаро миқёсда татбиқ этилиши кибержиноятларга қарши курашиш муаммосини ҳал қилиш учун етарли эмаслиги ахборот технологиялари ва дастурий таъминот соҳасидаги махсус кўникмаларни талаб этади.

Кибержиноятларга қарши курашиш тартибини регламентловчи ягона халқаро ҳужжат ишлаб чиқилмаган, аммо халқаро ҳамжамият минтақавий ҳамкорлик доирасида кибержиноятларга қарши курашда кибермакондаги субъектларнинг ҳаракатларини қонуний равишда тартибга солиш чораларини кўрмоқда.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР РЎЙХАТИ:

1. 2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics. URL: https://cybersecurityventures.com/cybersecurity-almanac-2019/.

2. Sachkov D.I., Smirnova I.G. Obespechenie informatsionnoi bezopasnosti v organakh vlasti [Ensuring Information Security in the Bodies of Power]. Irkutsk, Baikal State University of Economics and Law Publ., 2015. – P. 4.

3. Sindhu K.K., Kombade Rupali, Gadge Reena, Meshram B.B. Forensic Investigation Processes for Cyber Crime and Cyber Space. Proceedings of International Conference on Internet Computing and Information Communications, 2012, vol. 16. – P. 193.

4. Karpova D.N. Cybercrimes: a global issue and its solution. Vlast'= The Power, 2014. No. 8. – P. 46.

5. Schjolberg Stein. A cyberspace treaty – A United Nations convention or protocol on cybersecurity and cybercrime. Twelfth United Nations Congress on Crime Prevention and Criminal Justice. Salvador, Brazil, 12–19 April 2010. (Available at: http://cybercrimelaw.net/documents/UN_12th_Crime_Congress.pdf.)

6. См.: Голубев В.А. «Кибертерроризм» – миф или реальность? http://www.crime-research.ru/library/terror3.htm.

7. Варданян А.В. Расследование преступлений в сфере высоких технологий и компьютерной информации / А.В. Варданян, Е.В. Никитина. – М.: Юрлитинформ, 2007. – С. 15.

8. Huey L. Uppity civilians and cyber-vigilantes: The role of the general public in policing cyber-crime / L. Huey, J. Nhan, R. Broll // Criminology and Criminal Justice. – 2013. – Vol. 13, № 1. – P. 81

9. Якимова Е.М., Нарутто С.В. Международное сотрудничество в борьбе с киберпреступностью / Криминологический журнал Байкальского государственного университета экономики и права. 2016. – Т. 10. – № 2. – С. 371.

10. Берд К. Война со многими неизвестными / К. Берд // Компьютерра. – 2009. – № 20. – С. 26.

11. Химченко И.А. Информационное общество: правовые проблемы в условиях глобализации: дис. … канд. юрид наук: 12.00.13 / И.А. Химченко. – М., 2014. – С. 70.

12. Згадзай О.Э. Киберпреступность: факторы риска и проблемы борьбы / О.Э. Згадзай, С.Я. Казанцев // Вестник ГУ «Научный центр безопасности жизнедеятельности детей». – 2013. – № 4 (18), – С. 84.

13. Gradov A. The activities of the North Atlantic Treaty Organization in the sphere of cyber-security. Zarubezhnoe voennoe obozrenie = Foreign Military Review, 2014, no. 7, p. 13 (In Russian).

14. Smith R.G. Criminals on Trial / R.G. Smith, P. Grabosky, G. Urbas. – Cambridge University Press, 2004. – P. 60.

15. Жилина И.Ю. Киберпреступность и борьба с ней (сводный реферат) / И.Ю. Жилина // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 2, Экономика: реф. журн. – 2003. – № 1. – С. 144.

16. см. Конвенция об обеспечении международной информационной безопасности (концепция). URL: http://www.scrf.gov.ru/documents/6/112.html.

17. Смирнов А.А. Система борьбы с киберпреступностью в Европейском Союзе / А.А. Смирнов // Библиотека криминалиста. – 2012. – № 2 (3). – С. 267.

18. Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions «Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computerrelated Crime». Brussels, 26.1.2001. COM (2000) 890fi nal. URL: http://europa.eu.int/ISPO/eif/InternetPolicies Site/Crime/CrimeCommEN.html.

19. Европейская Конвенция по киберпреступлениям (преступлениям в киберпространстве): заключена в Будапеште 23 нояб. 2001 г. URL: http://conventions.coe.int/Treaty/RUS/Treaties/Html/185.htm.

20. Дополнительный протокол к Конвенции по киберпреступлениям в отношении криминализации деяний расистского и ксенофобского характера, осуществляемых при помощи компьютерных систем (подписан в г. Страсбург 28 янв. 2003 г.). URL: http://mvd.gov.by/main.aspx?guid=4593.

21. Химченко И.А. Информационное общество: правовые проблемы в условиях глобализации: дис. … канд.юрид наук: 12.00.13 / И.А. Химченко. – М., 2014. – С. 66.

22. Георгиева Р. Конвенция за киберпрестъпността / Р. Георгиева // Общество и право (София). – 2001. – № 11, с. 17

23. Талимончик В.П. Международно-правовое регулирование отношений в сфере информации: автореф.дис. … д-ра юрид. наук: 12.00.14 / В.П. Талимончик. – СПб., 2013. – С. 39.

24. Smirnov A.A. EU System of Fight against Cybercrime. Biblioteka kriminalista = Criminalist's Library, 2012, no. 2 (3), p. 268 (In Russian).

25. Волеводз А.Г. Учреждения и органы Европейского союза по судебному и полицейскому сотрудничеству: учеб. пособие / А.Г. Волеводз. – М.: Европ. учеб. ин-т при МГИМО(У) МИД России, 2010. – С. 88–89.

26. Eurojust casework in 2018 (Eurojust infographics). URL: http://www.eurojust.europa.eu/doclibrary/corporate/Pages/Eurojust-Infographics.aspx.

27. Кибертерроризм: угроза национальной и международной безопасности. URL: http://www.arms-expo.ru/news/archive/kibertmezhdunarodnoybezopasnosti14-03-2013-18-35-00/mezhdunarodnoy-bezopasnosti14-03-2013-18-35-00/.

28. Градов А. Деятельность Североатлантического союза в сфере кибербезопасности / А. Градов // Зарубежное военное обозрение. – 2014. – № 7. – С. 14.

29. Якимова Е.М., Нарутто С.В. Международное сотрудничество в борьбе с киберпреступностью / Криминологический журнал Байкальского государственного университета экономики и права. 2016. – Т. 10. – № 2. – С. 377.