UZBEKISTAN LAW REVIEW

ISSUE 2
2025

ЎЗБЕКИСТОН ҚОНУНЧИЛИГИ ТАҲЛИЛИ

UZBEKISTAN LAW REVIEW

ОБЗОР ЗАКОНОДАТЕЛЬСТВА УЗБЕКИСТАНА

ИЛМИЙ ТАҲЛИЛИЙ ЖУРНАЛ	SCIENTIFIC ANALYTICAL JOURNAL	НАУЧНО АНАЛИТИЧЕСКИЙ ЖУРНАЛ

2025

№2

Маълумот олиш учун қуйидагиларга мурожаат этиш сўралади:
Гулямов Саид Саидахрарович,
Рустамбеков Исламбек Рустамбекович
ТДЮУ, Халқаро хусусий ҳуқуқ кафедраси,
Ўзбекистон Республикаси, Тошкент ш., 100047,
Сайилгоҳ кўчаси, 35. Тел: 233-66-36

"Ўзбекистон қонунчилиги таҳлили"нинг электрон нусхаси Интернетдаги www.library-tsul.uz ёки www.lawreview.uz сайтида жойлаштирилган.

Журнал 2013 йилдан Ўзбекистон Республикаси Вазирлар Маҳкамасининг Олий Аттестация комиссияси журналлари рўйхатига киритилган.

2025 йилда нашр этилди.

ISSN 2181-8118

Масъул котиб: **И. Рустамбеков**
Нашриёт муҳаррири: **Н. Ниязова**
Техник муҳаррир: **Д. Козимов**
Лицензия № 02-0074
Босишга рухсат этилди – 28.06.2025
Нашриёт ҳисоб табоғи – 5
«IMPRESS MEDIA» босмахонасида босилди
Адади – 100 нусха.

ИЛМИЙ-ТАҲЛИЛИЙ ЖУРНАЛ ***2/2025***

Egamberdiyev Dilshodjon Alisherovich
yuridik fanlar bo‘yicha falsafa doktori
Toshkent davlat yuridik universiteti
Kiber huquq kafedrasi mudiri o‘rinbosari
dotsent v.b.

BMT VA XALQARO TASHKILOTLARDA KIBERTERRORIZMGA QARSHI KURASHNING XALQARO HUQUQIY MEXANIZMLARI

Аннотация. Данная статья посвящена анализу международных правовых механизмов борьбы с кибертерроризмом в рамках Организации Объединённых Наций (ООН) и других международных структур. В статье подчеркивается, что стремительное развитие цифровых технологий, наряду с предоставлением новых возможностей, порождает такие угрозы, как кибертерроризм. Автор отмечает, что термин «кибертерроризм» появился в 1980-х годах, однако отсутствие единого и четкого его определения создает определенные проблемы. В этой связи в статье подчеркивается отличие кибертерроризма от таких понятий, как «информационная война» и «кибепреступность», за счет его политической мотивированности. В статье выделяются два основных вида кибертерроризма: «чистый» кибертерроризм, предполагающий непосредственные атаки на компьютерные сети и критическую инфраструктуру, и использование интернета для пропаганды, вербовки, финансирования и координации преступной деятельности. Основная часть анализа сосредоточена на деятельности ООН в этой области, включая усилия Генеральной Ассамблеи и Совета Безопасности, направленные на создание глобальной культуры кибербезопасности и противодействие использованию интернета в террористических целях через принятие ряда резолюций. Также рассматривается роль других международных структур, таких как НАТО и «Большая восьмерка» (G8), в данной сфере. Несмотря на существующие усилия, подчеркивается отсутствие универсального международного договора по борьбе с кибертерроризмом, что препятствует эффективному сотрудничеству между государствами. В этой связи предлагается принятие под эгидой ООН конвенций, направленных на предотвращение кибертерроризма, борьбу с ним и противодействие финансированию терроризма посредством новых технологий.

Ключевые слова: кибертерроризм, международное право, ООН, кибербезопасность, борьба с терроризмом, международное сотрудничество, Совет Безопасности, Генеральная Ассамблея.

Abstract. This article is dedicated to the analysis of international legal mechanisms for combating cyberterrorism within the framework of the United Nations (UN) and other international organizations. The article highlights that the rapid development of digital technologies, while offering new opportunities, also gives rise to emerging threats such as cyberterrorism. The author notes that the term "cyberterrorism" emerged in the 1980s, yet the lack of a clear and universally accepted definition poses significant challenges. In this regard, the article delineates cyberterrorism from concepts such as "information warfare" and "cybercrime" by emphasizing its political motivations. Two primary forms of cyberterrorism are identified: "pure" cyberterrorism, which involves direct attacks on computer networks and critical infrastructure, and the use of the internet for propaganda, recruitment, financing, and coordination of criminal activities. The core of the analysis focuses on the UN’s efforts in this domain, particularly the initiatives of the General Assembly and the Security Council to foster a global cybersecurity culture and counter the use of the internet for terrorist purposes through the adoption of various resolutions. The article also examines the roles of other international entities, such as NATO and the Group of Eight (G8), in addressing this issue. Despite these efforts, the absence of a universal international treaty on combating cyberterrorism is highlighted as a significant barrier to effective interstate cooperation. In this context, the article proposes the adoption of conventions under the UN’s auspices aimed at preventing and combating cyberterrorism, as well as addressing the financing of terrorism through new technologies.

Keywords cyberterrorism, international law, UN, cybersecurity, counter-terrorism, international cooperation, Security Council, General Assembly.

Annotatsiya. Ushbu maqola Birlashgan Millatlar Tashkiloti (BMT) va boshqa xalqaro tuzilmalar doirasida kiberterrorizmga qarshi kurashning xalqaro huquqiy mexanizmlarini tahlil qilishga bag‘ishlangan. Maqolada raqamli texnologiyalarning jadal rivojlanishi ijobiy imkoniyatlar bilan bir qatorda kiberterrorizm kabi yangi tahdidlarni ham yuzaga keltirayotgani ta'kidlanadi. Muallif "kiberterrorizm" atamasining 1980-yillarda vujudga kelganini eslatib o‘tib, uning aniq va yagona ta'rifi yo‘qligi bilan bog‘liq muammolarga e'tibor qaratadi. Shu maqsadda maqolada kiberterrorizmning "axborot urushi" va "kiberjinoyat" kabi tushunchalardan siyosiy motivlari bilan farqlanishi ko‘rsatib berilgan. Maqolada kiberterrorizmning ikki asosiy turi ajratib ko‘rsatilgan: kompyuter tarmoqlari va muhim infratuzilmalarga bevosita hujum qilishni anglatuvchi "sof" kiberterrorizm hamda internetdan targ‘ibot, yollash, moliyalashtirish va jinoiy faoliyatni muvofiqlashtirish uchun foydalanish. Tahlilning asosiy qismi BMTning bu boradagi faoliyatiga qaratilgan bo‘lib, Bosh Assambleya va Xavfsizlik Kengashi tomonidan qabul qilingan bir qator rezolyutsiyalar orqali global kiberxavfsizlik madaniyatini yaratish va internetdan terrorchilik maqsadlarida foydalanishga qarshi kurashish borasidagi sa'y-harakatlar yoritilgan. Shuningdek, NATO va "Katta sakkizlik" (G8) kabi boshqa xalqaro tuzilmalarning ham bu sohadagi roli ko‘rib chiqilgan.

Mavjud sa'y-harakatlarga qaramay, kiberterrorizmga qarshi kurash bo‘yicha universal xalqaro shartnoma mavjud emasligi va bu holat davlatlar o‘rtasidagi hamkorlikka to‘siq bo‘layotgani ta'kidlanadi. Shu munosabat bilan, BMT shafeligida kiberterrorizmning oldini olish va unga qarshi kurashish hamda yangi texnologiyalar orqali terrorizmni moliyalashtirishga qarshi kurashish to‘g‘risidagi konvensiyalarni qabul qilish taklif etiladi.

Kalit so‘zlar: kiberterrorizm, xalqaro huquq, BMT, kiberxavfsizlik, terrorizmga qarshi kurash, xalqaro hamkorlik, Xavfsizlik Kengashi, Bosh Assambleya.

Kirish

Insonlarning kundalik hayotining eng yangi raqamli texnologiyalar bilan to'liq integratsiyalashganligi zamonaviy dunyoda hayotimiz tobora axborot makoniga aylanib borayotganligidan dalolatdir. Bugungi kunda, jadal rivojlanayotgan ilmiy va texnologik taraqqiyot dunyodagi deyarli har bir kishiga "Internet" tarmog'iga ochiq kirish imkoniyatiga ega bo'lgan kompyuter texnologiyalaridan bemalol foydalanishga imkonini yaratmoqda. Albatta, so'nggi yillarda keng miqyosdagi o'zgarishlar kelajakda yangi imkoniyatlar va istiqbollar uchun juda yaxshi imkoniyatlar yaratadigan yutuqdir. Bu yutuqlar nafaqat ijobiy jihatlari balki o'z navbatida, yangi zamnaviy ijtimoiy xavfli xatti-harakatlarni, xususan, kiberjinoyatlar, kiberterrorizm kabi salbiy jinoiy harakatlarni ham rivojlanishiga turtki bo'lmoqda. A.Pitinovaning ta'kidlaganidek, yangi axborot texnologiyalarini joriy etish, shuningdek, yagona virtual axborot makonini yaratish milliy va xalqaro xavfsizlikka yangi tahdidlar paydo bo'lishiga olib keladi[1]. Va bunday jinoyatlarni (kiberjinoyatlarni) amalga oshirish uchun katta miqdordagi moliyaviy mablag' talab etilmaydi. Insonlar uchun yaratilib kelinayotgan qator afzalliklar virtual ommaviy axborot vositalaridan ekstremistik, terroristik va kiberterror maqsadlarida amalga oshirish uchun joyda qulaylik yaratib bermoqda.

Bugungi kunda terrorizmning yangi bir ko'rinishi kiberterrorizm tushunchasi xalqaro huquq va milliy huquq tizimida juda ko'p uchrab turishi va kiberjinoyatlar xususuan kiberterrorizmni oldini olish bo'yicha bo'yicha bir qancha salmoqli ishlar olib borilayotganligi muhim hodisadir. "Kiberterrorizm" atamasi 1980-yillarning o'rtalarida hayotimizga kirdi, uning muallifi Amerika xavfsizlik va razvedka institutida katta ilmiy xodim bo'lib ishlagan Barri Kollin edi. Bu atama muallif tomonidan virtual makonda terrorchilik harakatlarini aniqlash va faqat kelajak uchun bashoratlar uchun ishlatilgan. Kiberterrorizm davlatlarning bank, transport va energetika tizimlari uchun, ayniqsa hukumat, iqtisodiyotning davlat va xususiy sektorlari, axborot uchun jiddiy tahdiddir.

"Kiberterrorizm"ni aniqlash bo'yicha uslubiy muammolar, birinchi navbatda, terrorizmning bunday shaklini axborot urushidan yoki axborot qurollaridan foydalangan holda noqonuniy harakatlardan ajratish ba'zan qiyin bo'lganligi bilan bog'liq. Ba'zilar haqiqiy kiberterror hujumi hali sodir bo'lmagan deb da'vo qilsa, boshqalari terrorchilar allaqachon internetdan o'z manfaatlari uchun foydalanmoqda, deb ta'kidlaydilar. Ushbu kelishmovchilikning manbai "terrorizm" va "kiberterrorizm" ning aniq ta'rifi yo'qligidir.

2. Material va metodlar

Ushbu tadqiqotda BMT va xalqaro tashkilotlarda kiberterrorizmga qarshi kurashning xalqaro huquqiy mexanizmlarini o'rganish uchun quyidagi metodlar qo'llanildi. Tarixiy-huquqiy tahlil metodi orqali kiberterrorizm tushunchasining paydo bo'lishi va rivojlanish bosqichlari o'rganildi. Qiyosiy-huquqiy tahlil metodi yordamida turli xalqaro tashkilotlar tomonidan ishlab chiqilgan ta'riflar va yondashuvlar solishtirildi. Tizimli tahlil metodi orqali kiberterrorizmga qarshi kurashning xalqaro huquqiy mexanizmlari yaxlit tizim sifatida ko'rib chiqildi.

Tadqiqot obyekti sifatida BMT Bosh Assambleyasi va Xavfsizlik Kengashi tomonidan qabul qilingan rezolyutsiyalar, xalqaro konvensiyalar, Stanford universiteti loyihasi va boshqa xalqaro tashkilotlarning tegishli hujjatlari tanlab olindi. Material sifatida 2000-yildan 2019-yilgacha bo'lgan davrda qabul qilingan asosiy xalqaro huquqiy hujjatlar tahlil qilindi. Hujjatlar tahlili metodi orqali rezolyutsiyalar va konvensiyalarning mazmuni chuqur o'rganildi va normativ-huquqiy tahlil metodi orqali xalqaro huquq normalarining samaradorligi baholandi.

3. Tadqiqot natijalari

Umuman terror so'zi lotincha "terrere" so'zidan kelib chiqqan bo'lib, "qo'rqitish, zo'ravonlik, vahima uyg'otish"degan ma'noni anglatadi[2]. Odatda, terrorizmni belgilash muayyan siyosiy maqsadga bog'liq va yo'naltirilgan bir qator terroristik harakatlarni talab qiladi. Bozdemirning fikricha, "terrorizm siyosiy maqsadlarda o'zini uyushgan, tizimli va uzluksiz terrordan foydalanishni o'z ichiga olgan usul bilan aniqlanadigan strategik yondashuvdir"[3].

D.Denning terrorizmni "ko'pincha mafkuraviy, siyosiy sabablarga ko'ra turli jamiyat a'zolari yoki hukumatlarni qo'rqitish, ularni majburlash niyatida shaxs yoki uyushgan guruh tomonidan insonlarga, ularning mulkga nisbatan kuch yoki zo'ravonlikni noqonuniy qo'llash, tahdid qilish"deb ta'riflaydi[4]. S.E.Serkerov terrorizmga ta'rif berishda bevosita uning maqsadlari bilan ajratadi, xalqaro munosabatlarga, xalqaro huquqiy tartibotga putur yetkazish; davlatga, millatga, xalqaro tashkilotga qarshi harakatlar deb qaraydi. Tadqiqotchi xorijiy elementni o'z ichiga olgan aksiyalar har doim ham xalqaro toifaga kirishi shart emas, deb to'g'ri ta'kidlaydi[5].

F.Reynaresning fikricha, terrorizmning bir davlat chegarasidan tashqariga chiqadigan ikkita variantini ajratib ko'rsatadi: transmilliy (umumiy toifa) va xalqaro – bu esa oqibatlari jihatidan eng xavfli, og'ir shakl hisoblanadi[6]. F.Reynares xalqaro terrorizmning o'ziga xos belgilarini quyidagicha taklif qiladi: uning maqsadlari – mintaqalar va global miqyosda hokimiyatning tuzilishi va taqsimlanishi; ko'p sonli mamlakatlar va geosiyosiy hududlarda faoliyat yurituvchi tashkiliy tarmoq tuzilmasi tizimiga ataylab ta'sir qilish. Muallif bunday tuzilmaga neosalafiylar

(salafiylarning global jihodi) harakatini misol sifatida keltiradi[7].

Albatta kiberterrorizm terrorizmning yangi shakli bo'lib, kompyuter tarmoqlaridan foydalanish va yuqori texnologiyalar yutuqlari natijasida shakllangan. Globallashuv natijasida bu muammoning ijtimoiy xavfliligi xalqaro miqyosda tan olindi. D.Denning kiberterrorizmni terrorizm va kiber makonning yaqinlashuvi sifatida belgilaydi. Uning fikricha "kiberterrorizm bu hukumatlar yoki aholini siyosiy, ijtimoiy, mafkuraviy maqsadlarga erishish uchun qo'rqitish, majburlashni kompyuterlar, tarmoqlar va ularda saqlanadigan ma'lumotlarga noqonuniy hujumlar va hujum tahdidlari orqali amalga oshirishdir"[8]. K.Bradley va M.Gulatilar ham bevosita Denning fikrini qo'llab qo'vattalab kiberterrorizmni oddiy terrorizmdan ajratib turadigan muhim narsa bu albatta kompyuter tarmoqlaridan foydalanish (asosan Internetga asoslangan jinoiy harakatlar hisoblanadi)[9] deb ko'rsatib o'tishadi.

V.Golubev kiberterrorizm bu kompyuter ma'lumotlari, tizimi yoki tarmog'iga qasddan qilingan hujum va uning maqsadi davlat va xalqaro xavfsizlikka tahdid solish, jamiyatni qo'rqitish yoki biron bir mintaqada harbiy mojaroni qo'zg'atishdir deb ta'rif bergan[10]. A.Panenkov, M.Efremova, kiberterrorizm siyosiy yoki ijtimoiy masalalarni hal qilishda hokimiyat organlariga bosim o'tkazish uchun kompyuter tizimlari, tarmoqlari yoki ulardagi ma'lumotlarga qaratilgan noqonuniy xatti-harakatlar deb ta'rif berishadi[11].

R.Absatarovning fikricha, kiberterrorizm deganda siyosiy maqsadni ko'zlab xalqaro yoki milliy guruhlar tomonidan aholi yoki hukumatga siyosatni o'zgartirishga ta'sir ko'rsatish maqsadida kompyuter tarmoqlaridan qurol yoki nishon sifatida foydalanish, zarar yetkazish yoki tahdid qilish va vahima uyg'otish tushunilishi mumkin[12] deb ta'kidlaydi.

2000-yilda Stenford universitetining "Kiberjinoyat va terrorizmga qarshi kurashni kuchaytirish to'g'risida"gi xalqaro konvensiyasi loyihasida keltirildi. Unga ko'ra kiberterrorizm "…kompyuter tarmoqlaridan zo'ravonlikni, terrorni targib qilish, jamiyatda qo'rquvni uyg'otish uchun qasddan foydalanish yoki foydalanish bilan tahdid qilish, bunday foydalanish jamiyat va insonlar tan jarohatlari yetkazishiga yoki o'limiga, turli muluk turlariga jiddiy zarar yetkazishga, turli fuqarolik tartibsizliklarni kelrtirib chiqarishiga yoki muhim iqtisodiy zararga olib kelishi sabab bo'lsa…[18]" deb kiberterrorizmning sabablari va belgilari sanab ko'rsatildi.

Kiberterrorizmning ikkita asosiy turi mavjud. Kiberterrorizmning birinchi turi -bu "sof" deb ataladigan kiberterrorizm bo'lib, bu yerda terroristik harakatlar kompyuterlar va kompyuter tarmoqlari yordamida amalga oshiriladi. Kiberterrorizmning ikkinchi turi - terroristik guruhlar tomonidan global axborot makonidan tashkiliy-kommunikatsiya maqsadlarida foydalanishdir.

Universal tashkilot sifatida BMTning kiberxavfsizlikni ta'minlash bilan bog'liq harakatlari XXI asrning boshlariga, to'g'ri keladi. Bunda BMTning asosiy organlari tomonidan bir qancha rezolyutsiyalar qabul qilindi. Birlashgan Millatlar Tashkiloti Bosh Assambleyasining 2000-yil 4-dekabrda qabul qilingan rezolyutsiyasida[23] davlatlar axborot texnologiyalaridan jinoiy faoliyatdan foydalanishga qarshi kurashishning turli usullari ko'rib chiqilgan. Shuningdek 2002-yilda qabul qilingan 57/239-sonli rezolyutsiya[24] qabul qilindi. Ushbu rezolyutsiya bilan global kiberxavfsizlik madaniyatini yaratish belgilab berildi.

BMT Bosh Assambleyasi 57/239-sonli rezolyutsiyaning mantiy davomi sifatida 2004-yil 30-yanvarda BMT Bosh Assambleyasining 58/199-son rezolyutsiyasi[25] qabul qilindi. Ushbu rezolyutsiyada ham bevosita kiberxavfsizlikning global madaniyatini shakllantirish zarurligi tan olindi. 2005-yilda o'tkazilgan jahon sammitida yakuniy hujjati sifatida Bosh Assambleya 2006-yilda qabul qilingan Global terrorizmga qarshi strategiyasi[26] qabul qilindi.

Bugungi kungacha Xavfsizlik Kengashi terrorizmga qarshi kurash bo'yicha bir qancha rezolyutsiyalar qabul qildi. Xususan 2005-yilda Xavfsizlik Kengashi xalqaro chegaralar xavfsizligi sohasida xalqaro hamkorlikni mustahkamlashga qaratilgan 1624-sonli rezolyutsiyani qabul qildi. 2013-yilda 2129-sonli Rezolyutsiya qabul qilindi. Ushbu rezolyutsiyaga ko'ra: "terrorizm va axborot-kommunikatsiya texnologiyalari, xususan, Internet tarmog'idan, aloqa o'rnatib va bunday aloqalardan foydalanib axborot-texnologiyalar orqali terroristik harakatlarni qo'zg'atish, ularni jalb qilish, moliyalashtirish, rejalashtirish orqali terroristik harakatlarni sodir etish va ularga yordam berish…[30]" deb aniq kiberterrorizmning sodir etilishiga qarshi kurashni taqiqlashga chaqirildi.

2014-yilda qabul qilingan Xavfsizlik Kengashining 2178-sonli rezolyutsiyasi[31] bilan "…a'zo davlatlar terrorchilarning terroristik harakatlarni qo'llab-quvvatlashga undash uchun axborot-texnologiya, aloqa va elektron resurslardan foydalanishiga yo'l qo'ymaslik uchun milliy choralarni ko'rishda birgalikda harakat qilish…"ga chaqirildi. Xavfsizlik Kengashi kiberterrrizmga qarshi kurash bo'yicha 2016-yilda 2322-son[32] rezolyutsiya, 2016-yilda 2331-son[33] rezolyutsiya, 2017-yilda 2341-son[34] rezolyutsiya va 2017-yilda 2396-son[35] rezolyutsiyalar qabul qildi. Xavfsizlik Kengashining 2019-yilda qabul qilimgan 2469-son[36] rezolyutisyasi orqali terrorchilik maqsadlarida mablag' yig'ish uchun turli electron to'lov platformalaridan foydalanish oldini olish talab etildi.

4. Tadqiqot natijalari tahlili

BMTning asosiy organlari (Bosh Assambleya va Xavfsizlik Kengashi)dan tashqari BMTning ixtisoslashgan organlari tomonidan ham kiberterrorizmga qarshi kurash bo'yicha ayrim harakatlar amalga oshirildi. Xususan, Avstriyaning Vena shahridagi Birlashgan Millatlar Tashkilotining Giyohvand moddalar va jinoyatchilik bo'yicha idorasining kongressida Birlashgan Millatlar Tashkilotining terrorizmning oldini olish sektorini tashkil etdi. 2005-yilda Tailandning Bangkok shahrida bo'lib o'tgan jinoyatchilikka qarshi kurash Kongressida maxsus seminarda kompyuter jinoyati bilan bog'liq masalalar,

maxsus qo'mitada esa terrorizmga qarshi kurash bo'yicha xalqaro huquqiy hujjatlarning kuchli va zaif tomonlari muhokama qilindi[37].

Kiberxavfsizlikni ta'minlash va kiberjinoyatchilikka qarshi kurashni eng samarali amlga oshirib kelayotgan BMTning ixtisoslashgan organi bu Jenevada joylashgan Xalqaro telekommunikatsiya Ittifoqi hisoblanadi. Ushbu tashkilot 2006-yil may oyida 2005-yilda Tunisda o'tkazilgan Axborot jamiyati bo'yicha butunjahon sammitning davomi sifatida Global kiberxavfsizlik bo'yicha hamkorlikni rivojlantirish uchun maslahatlashuv tadbirini tashkil etdi.

Xalqaro huquqda BMT va uning ixtisoslashgan tashkilotlaridan tashqari yana bir nechta xalqaro tashkilotlar kiberxavsizlikni ta'minlash va kiberjinoyatlarning barcha turlariga qarshi kurashni amalga oshirib kelmoqda. Xususan, Shimoliy Atlantika shartnomaviy tashkiloti (keyingi o'rinlarda NATO) kiberhujumlarga qarshi kurashni boshlaganiga u qadar uzoq vaqtni qamrab olmaydi. 2007-yilda Estoniyaga qilingan kiberhujum NATO tashkilotining kiberjinoyatlarga qarshi kurash bo'yicha "kibernetik ta'limot va keng qamrovli kibernetik strategiyaga ega emasligini" va ko'rsatib qo'ydi[38].

1997-yilda G8 davlatlari guruhi yuqori texnologiyali jinoyatchilikka qarshi kurash bo'yicha kichik guruhni tashkil etdi va kompyuter jinoyatlariga qarshi kurashning o'nta tamoyilini ishlab chiqdi va qabul qildi. Bundan ko'zlangan asosiy maqsad jinoyat sodir etgan har qanday shaxs dunyoning hech bir joyida "xavfsiz boshpana" olmasligi edi. G8 davlatlari guruh bilan 40 ortiq davlat hamkorlik qilishni yoqlab chiqishdi va guruh tomonidan 24/7 xizmat ko'rsatish tarmog'i ishlab chiqildi.

Tahlillar natijasida ma'lum bo'ldiki, kiberterrorizm va axborot urushi o'rtasida sezilarli farq bor. Kiberterrorizm deganda submilliy guruhlar yoki maxfiy agentlar yoki shaxslarning tinch maqsadlarga nisbatan zo'ravonlikka olib keladigan axborot va kompyuter tizimlari, kompyuter dasturlari va ma'lumotlariga qasddan, siyosiy sabablarga ko'ra hujumlari tushuniladi. Axborot urushi ancha eski tushuncha bo'lib "davlatlar yoki ularning organlari tomonidan axborot va kompyuter tizimlari, kompyuter dasturlari va ma'lumotlariga qarshi rejalashtirilgan hujum" hisoblanadi.

Bugungi vaqtda BMT tomonidan transmilliy jinoyatlarning 17 ta turi bevosita sanab ko'rsatildi. Ularga: terrorizm; madaniy yodgorliklar va san'at asarlarini o'g'irlash; intellektual mulk huquqini o'g'irlash; noqonuniy qurol-yarog' savdosi; havo kemalarini olib qochish; dengiz qaroqchiligi; yer ustki transport vositalarini qo'lga olish; sug'urtalangan firibgarlik; kompyuter jinoyatchiligi; ekologiya sohasidagi jinoyatlar; odam savdosi; inson tana a'zolarini noqonuniy sotish; giyohvand vositalar va psixotrop moddalarning noqonuniy savdosi; soxta (qalbaki) bankrotlik; tijoratga noqonuniy suqulib kirish; korrupsiya, siyosiy partiya vakillari va mansabdor shaxslarni sotib olish; jinoiy yo'l bilan topilgan daromadlarni legallashtirish ("pul yuvish") kabi jinoyatlari kiradi[22].

5. Xulosalar

Yuqoridagi tahlillar natijasida shuni qayd etishimiz kerakki kiberjinoyatlar va kiberterrorizmga qarshi kurash bo'yicha BMT tomonidan yagona xalqaro hujjat qabul qilinmagandir. Natijada, bu jinoyatlarga qarshi kurashni amalga oshirishda davlatlar o'rtasida turli tushunmovchiliklar keltirib chiqarmoqda. Fikrimizcha BMT tomonidan "Kibberterrorizmni oldini olish va unga qarshi kurash to'g'risida"gi Konvensiya va "Kriptovalyutalar va boshqa yangi texnologiyalar orqali terrorizmni moliyalashtirishga qarshi kurash to'g'risida"gi Konvensiyalar qabul qilish davr talabi bo'lib qolmoqda.

"Kibberterrorizmni oldini olish va unga qarshi kurash to'g'risida"gi Konvensiya terroristik guruhlar tomonidan kiberhujumlarni targib qilish, kiberhujumlarga sodir etishga yollash, targib qilish, kiber makon orqali turli terroristik harakatlarni moliyalashtirish uchun mablag' yig'ish va kibermakon orqali insonlarni qo'rqitish, ularni qaram qilib qo'yish, shaxslarning shaxsiy ma'lumotlarni o'zlashtirish va ulardan keng foydalanish kabi jinoiy tahdidlar va harakatlarga qarshi kurashish uchun huquqiy asos yaratishi mumkin.

Kiberterrorizmning global ta'sirini hisobga olgan holda, Birlashgan Millatlar Tashkiloti xalqaro tinchlik va xavfsizlikni saqlashning markaziy organi sifatida ushbu tahdidga qarshi kurashda hal qiluvchi rol o'ynaydi. Biroq, mavjud xalqaro huquqiy mexanizmlar to'liq samarali emas va yangi texnologik tahdidlarga moslashtirilishi zarur. Kiberterrorizm bu ko'p qirrali hodisa sifatida tushunilishi kerak bo'lgan tushunchadir, va u virtual makon bilan bog'langan hujum bilan ifodalanib, insonlarning hayoti yoki sog'ligi uchun xavf tug'diradi yoki boshqa jiddiy oqibatlarga olib keladigan, ko'pincha bunday harakatlar jamoat xavfsizligini buzish, aholini qo'rqitish, infratuzilmaga zarar yetkazish va boshqa shu kabi harakatlar bilan bog'liq hodisalar deb ta'rif berish maqsadga muvofiq bo'ladi.

Список использованных литературы:

[1] Питинова А.С. Актуальные вопросы противодействия кибертерроризму // Право: история, теория, практика: материалы VI Международной научной конференции. – СПб: Свое издательство, 2018. – С. 31.

[2] P. Wilkinson, Political Terrorism, London, 1974.

[3] M. Bozdemir, "What Is Terror and Terrorism?," School of Political Sciences Press and Publication College, 1981, p. 17

[4] D. Denning, "Cyber terrorism. Testimony before the Special Oversight Panel on Terrorism," Committee on Armed Services U.S. House of Representatives, Georgetown University, May 2000. http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

[5] Серкеров С.Э. Криминологические проблемы международного терроризма: дис. ... канд. юрид. наук: 12.00.08: Махачкала 2004. С. 54, 60.

[6] Drodríguez-Villasante Prieto J. L. Lucha Contra El Terrorismo Y Derecho Internacional. P. 42.

[7] Reinares F. Conceptualising International Terrorism …

[8] D. Denning, "Cyber terrorism. Testimony before the Special Oversight Panel on Terrorism," Committee on Armed Services U.S. House of Representatives, Georgetown University, May 2000. http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

[9] Curtis A. Bradley & Mitu Gulati, Customary International Law and Withdrawal Rights in an Age of Treaties, 21 DUKE J. COMP. & INT'L L. 1 (2010)

[10] Голубев В. А. Кибертерроризм — угроза национальной безопасности / http://www.crime-research.ru/articles/Golubev_ Cyber_Terrorism/

[11] Ефремова М. А. Уголовно-правовое обеспечение кибербезопасности // Информационное право. 2015. № 5. С. 10–13. Паненков А. А. Кибертерроризм как реальная угроза национальной безопасности России // Право и кибербезопасность. 2018. № 1. С. 12–19.

[12] Абсатаров Р. Р. Противодействие компьютерному терроризму // Современная юриспруденция: актуальные вопросы, достижения и инновации. Сборник статей VI Международной научно-практической конференции. 2018. С. 172–174.

[13] Абдулатипов А.М. Понятие информационного терроризма // Юридический вестник Дагестанского государственного университета. – 2019. – N 2. – С. 106

[14] Диденко А.И. Понятие и место кибертерроризма в уголовном праве России // Отечественная юриспруденция. – 2016. – N 9 (11). – С. 5

[15] Хачидогов Р.А. Понятие и проблемы противодействия кибертерроризму // Журнал прикладных исследований. – 2021. – N 3. – С. 74-78

[16] Белкин Р.С. Курс криминалистики.Т. 3. – М., 1997. – С. 190.

[17] Белкин Р.С. Криминалистика: Учебник для вузов. – М., 2001. – С. 126.

[18] Abraham D. Sofaer et al., A Proposal for an International Convention on Cyber Crime and Terrorism 26 (Aug. 2000) (paper presented at the Stanford Conference at Stanford University), available at http://iis-db.stanford.edu/pubs/11912/sofaer goodman.pdf.

[19] Васильев М. Кибертерроризм как элемент гибридной войны [Электронный ресурс] // Геополитика. 2018. № 5. URL: https://www.geopolitica.ru/article/kiberterrorizm-kak-element-gibridnoyvoyny (дата обращения: 15.04.2020).

[20] Бураева Людмила Александровна КИБЕРТЕРРОРИЗМ КАК НОВАЯ И НАИБОЛЕЕ ОПАСНАЯ ФОРМА ТЕРРОРИЗМА Проблемы экономики и юридической практики 2'2017 С 189

[21] Н.О.Мороз МЕЖДУНАРОДНО-ПРАВОВАЯ КВАЛИФИКАЦИЯ КИБЕРТЕРРОРИЗМА «ИСТОРИЧЕСКИЕ НАУКИ. ЮРИДИЧЕСКИЕ НАУКИ». 2016. Т. 2. № 2 (6) С.81

[22] N.O.Hamidov Ayrim transmilliy uyushgan jinoyatlar uchun javobgarlik: jinoyat-huquqiy va kriminologik jihatlar. Yuridik fanlar bo'yicha falsafa doktori dissertatsiyasi Toshkent – 2022. B. 29.

[23] Resolution adopted by the General Assembly Combating the criminal misuse of information technologies A/Res/55/63 // https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf

[24] Resolution adopted by the General Assembly Creation of a global culture of cybersecurity A/RES/57/239 // https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf

[25] Создание глобальной культуры кибербезопасности и защита важнейших информационных инфраструктур A/RES/58/199 // https://documents.un.org/doc/undoc/gen/n03/506/54/pdf/n0350654.pdf?token=NSdmCUSWmuE8j5sTuQ&fe=true

[26] The Strategy was adopted by the General Assembly on September 8, 2006 (A/res/60/288)

[27] BMT Ustavi https://unic.un.org/aroundworld/unics/common/documents/publications/uncharter/charter_Uzbek.pdf

[28] Ian Johnstone, 'Legislation and Adjudication in the UN Security Council: Bringing Down the Deliberative Deficit', 102 Am. J. Int'l L. 275 (2008), at p. 283.

[29] Resolution 1624 (2005) Adopted by the Security Council at its 5261st meeting, on 14 September 2005 S/RES/1624 of 14 September 2005 // http://unscr.com/en/resolutions/doc/1624

[30] Резолюция 2129 (2013), принятая Советом Безопасности на его 7086-м заседании 17 декабря 2013 года S/RES/2129 (2013) // https://documents.un.org/doc/undoc/gen/n13/624/39/pdf/n1362439.pdf?token=eVVgLgU0w CEQoF1uzH&fe=true

[31] Резолюция 2178 S/RES/2178 (2014) // https://documents.un.org/doc/undoc/gen/n14/548/01/pdf/n1454801.pdf?token=AJBEuviHtiNKQorSQx&fe=true

[32] Резолюция 2322 (2016) S/RES/2322 // https://documents.un.org/doc/undoc/gen/n16/433/58/pdf/n1643358.pdf?token=Zo2OYZgnwIaxPhvzEr&fe=true

[33] Резолюция 2331 S/RES/2331 (2016) // https://documents.un.org/doc/undoc/gen/n16/451/62/pdf/n1645162.pdf?token=YSQqZo5iHzjIqHP0jL&fe=true

[34] Резолюция 2341 S/RES/2341 (2017) // https://documents.un.org/doc/undoc/gen/n17/038/61/pdf/n1703861.pdf?token=eRwyhR9iK0A9ZmFuu4&fe=true

[35] Резолюция 2396 S/RES/2396 (2017) // https://documents.un.org/doc/undoc/gen/n17/460/27/pdf/n1746027.pdf?token=wKVEyDxs7iPCthC6fG&fe=true

[36] Resolution 2469 S/RES/2469 (2019) // https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_res_2469.pdf

[37] Elektron resurs: http://www.unodc.org/unodc/crime_congress_11/documents.html

[38] Rex B. Hughes, NATO and Cyber Defence: Mission Accomplished?, ATLANTISCH PERSPECTIEF, Apr. 2009, at 1, available at

http://www.atlcom.nl/site/english/nieuws/wpcontent/Hughes.pdf.

[39] Scott J. Shackelford, Estonia Two-and-aHalf Years Later: A Progress Report on Combating Cyber Attacks, J. INTERNET L. 5 (forthcoming), available at http://ssrn.com/abstract=1499849.