KIBERTAHDID - FALSAFIY TADQIQOT OB'EKTI SIFATIDA

Batirov Farxod Avazovich
O'zbekiston Respublikasi Jamoat xavfsizligi universiteti O'quv-uslubiy boshqarmasi, o'quv jarayonini rejalashtirish bo'limi boshlig'i
e-mail: Farxod-batirov@mail.ru

ANNOTATSIYA

Maqolada XXI asrga kelib kibermakonning rivojlanishi natijasida uning ijobiy jihatlari bilan birgalikda, salbiy jihatlari ham kuchayib borayotganligi, bunday holat o'z navbatida kiberxavfsizlikka e'tiborni kuchaytirishni talab etilishini, chunki kiberxavfsizlikka tahdid solayotgan kiberjinoyat, kibertahdid, kiberurush va kiberhujum kabilar inson ma'naviy-ruhiy olamini izdan chiqarayotganli, shuningdek, ushbu xavf-hatarlarga qarshi kurashishning tizimli chora-tadbirlari yoritilgan.

Kalit so'zlar. *Ma'naviy tarbiya, axloqiy tarbiya, kiberjinoyat, kibertahdid, kibermakon, kiberurush, kiberhujum, kiberxavfsizlik.*

КИБЕРУГРОЗА КАК ОБЪЕКТ ФИЛОСОФСКОГО ИССЛЕДОВАНИЯ

Батиров Фарход Авазович
начальник отдела планирования учебного процесса учебно-методического управления, Университета общественной безопасности Республики Узбекистан
e-mail: Farxod-batirov@mail.ru

АННОТАЦИЯ

В статье в результате развития киберпространства к XXI веку усиливаются его положительные стороны, а также выделяются его отрицательные стороны, разрушающие духовный мир, а также системные меры борьбы с этими опасностями.

Ключевые слова. *Духовное образование, нравственное воспитание, киберпреступность, киберугроза, киберпространство, кибервойна, кибератака, кибербезопасность.*

CYBER THREAT AS AN OBJECT OF PHILOSOPHICAL RESEARCH

Batirov Farhod Avazovich
Head of the educational process planning department of the educational and methodological department of the University of Public Security of the Republic of Uzbekistan
e-mail: Farxod-batirov@mail.ru

ABSTRACT

The article, as a result of the development of cyberspace by the 21st century, enhances its positive aspects, and also highlights its negative aspects that destroy the spiritual world, as well as systemic measures to combat these dangers.

Key words. *Spiritual education, moral education, cybercrime, cyberthreat, cyberspace, cyberwar, cyberattack, cybersecurity.*

KIRISH

Ma’naviy tarbiya nuqtai nazaridan, yoshlarni kiber tahdidlarga nisbatan hushyor va axloqiy jihatdan barqaror qilib tarbiyalash muhim ahamiyat kasb etadi. Ma’naviy tarbiya yoshlarni nafaqat texnologik bilim bilan qurollantirishi, balki ular kibermakon axloqiy me’yorlarga rioya qilish, shaxsiy ma’lumotlarni himoya qilish, noto‘g‘ri axborotga qarshi kurashish va boshqalarning huquqlariga hurmat bilan munosabatda bo‘lish bo‘yicha o‘rgatilishi kerak. Axloqiy tarbiya, ayniqsa, ma’lumotlar daxlsizligini himoya qilishda va kibertahdidlarning zararlarini kamaytirishda muhim vosita sifatida qaraladi. Shu ma’noda, kiberhujumlarning oldini olish uchun nafaqat texnik vositalar, balki axloqiy-ruhiy himoya ham zarur bo‘lib, bu insonlarning axloqiy immunitetini oshirish orqali amalga oshiriladi. Shuningdek, kibertahdidlarning turli madaniy va geosiyosiy kontekstlarda qanday shakllanishi va unga qanday javob berish axloqiy masalalarni ham keltirib chiqaradi. Kiberjinoyatlar yoshlar (ijtimoiy) dunyo qarashining madaniy va axloqiy qoidalarning buzilishi bo‘lib, bu jamiyatda tartib va barqarorlikka tahdid soladi. Shu boisdan, yoshlarni o‘z milliy va global axloqiy qadriyatlarni hurmat qilishga, kibermakon ichida axloqiy tamoyillarga amal qilishga o‘rgatish bugungi kunda yanada muhimroq bo‘lib qoldi. Kibertahdidlarni bartaraf etishda ma’naviy-axloqiy tarbiya axloqiy qadriyatlarni targ‘ib qilish, insonlar orasida o‘zaro ishonch va hurmatni mustahkamlash, axborot madaniyatini rivojlantirish yo‘lida muhim rol o‘ynaydi.

Chunki kibermakonda insonlarning axloqiy va ma’naviy qadriyatlarini mustahkamlash va himoya qilish zarurati kun sayin oshib bormoqda, bu sohadagi kiberxavf eng katta tahdidlardan biridir. Kibertahdidlarning axloqiy jihatlari kibermakonda ma’naviy mas’uliyat va javobgarlikni aniqlashga olib keladi. Kiberhujumlar oqibatida paydo bo‘ladigan axloqiy muammolarni, kiberjinoyatchilar va ularning maqsadlari, shuningdek, shaxs-davlat va tashkilotlarning kiberhujumlarga qarshi kurashish borasidagi o‘zlarining axloqiy mas’uliyatlarini anglashlari va raqamli xavfsizlik choralarini mustahkamlashlari kerak. Masalan, davlatlar kiberurush vositalaridan foydalangan holda boshqa davlatlar ustidan kuchli nazorat o‘rnatishga harakat qilishlari mumkin. Shu bilan birga, korporatsiyalar katta hajmdagi ma’lumotlarni to‘plash orqali shaxsiy hayotga xavf tug‘diradi. Bu holat insonlar va

texnologik tizimlar o‘rtasidagi kuchlar muvozanatiga falsafiy munosabatni talab qiladi.

TADQIQOT METODOLOGIYASI (RESEARCH METHODOLOGY). Raqamli makon epistemologik masalalarni ham keltirib chiqaradi. Faylasuflar raqamli sohada haqiqiy axborotni noto‘g‘ri ma’lumotlardan ajratish masalasini o‘rganadilar. Kiberjinoyatlar, noto‘g‘ri axborot tarqatish va manipulyatsiya qilish haqiqat tushunchamizni buzishi mumkin. Shu sababli, ma’naviy tarbiya doirasida haqiqatni izlash, axborot manbalarini sinchkovlik bilan tahlil qilish va sog‘lom tanqidiy fikrlash qobiliyatlarini rivojlantirish muhim hisoblanadi. Kibermakonda texnologiya va inson o‘rtasidagi ontologik bog‘liqlikni o‘rganish axloqiy tuzilmalarni yanada murakkablashtiradi. Avtonom tizimlar, sun’iy intellekt va boshqa raqamli vositalar kibermakonni boshqarishda bevosita ishtirok etadi va bu texnologiyalar inson niyatlari va axloqiy printsiplarga qanday ta’sir ko‘rsatishini o‘rganishni talab qiladi. Ushbu tahlillar texnologiyalarning axloqiy muammolarini yanada chuqurroq tushunishga yordam beradi.

Kibertahdidlar jamiyatning siyosiy va ijtimoiy tuzilmalariga ham katta ta’sir ko‘rsatadi. Kibermakonda adolat, tenglik va erkinlik kabi qadriyatlar qanday saqlanadi? Suverenitet, demokratiya va shaxsiy hayotni himoya qilish kabi tamoyillar kibermakondagi murakkab ijtimoiy jarayonlar bilan bog‘liq. Masalan, kuzatuv va monitoring texnologiyalari inson erkinliklarini cheklashi mumkin, bu esa jamiyatda erkinlik va adolatga oid savollarni keltirib chiqaradi. Falsafiy nuqtai nazardan, kibertahdidlarning insoniyat sivilizatsiyasiga yetkazishi mumkin bo‘lgan ekzistensial xavflar ham alohida o‘rganiladi. Texnologiyaning nazoratsiz rivojlanishi va kibermakondagi xavflarning kattaligi inson hayoti uchun jiddiy xavflarni keltirib chiqarishi mumkin. Faylasuflar texnologiyaning ushbu jihatlarini o‘rganish orqali, insoniyat kelajagi va hayoti uchun axloqiy javobgarlik masalalarini yoritib beradilar.

TAHLIL VA NATIJALAR (ANALYSIS AND RESULTS).

Kibertahdidlarni falsafiy va axloqiy nuqtai nazardan o‘rganish, texnologiya va axloq o‘rtasidagi munosabatni yanada chuqurroq tushunishga yordam beradi. Kibermakonda ma’naviy va axloqiy tarbiya orqali kiberxavfsizlikni kuchaytirish jamiyat va shaxslar uchun o‘ziga xos yo‘nalish bo‘lib xizmat qiladi. Bu jarayon kibermakondagi axloqiy va ma’naviy mas’uliyatni oshirish, texnologiyalarni insoniy qadriyatlar bilan uyg‘unlashtirishga qaratilgan bo‘lishi zarur. Shu o‘rinda kibertahdid tushunchasining etimologik jihatlariga to‘htalib o‘tsak.

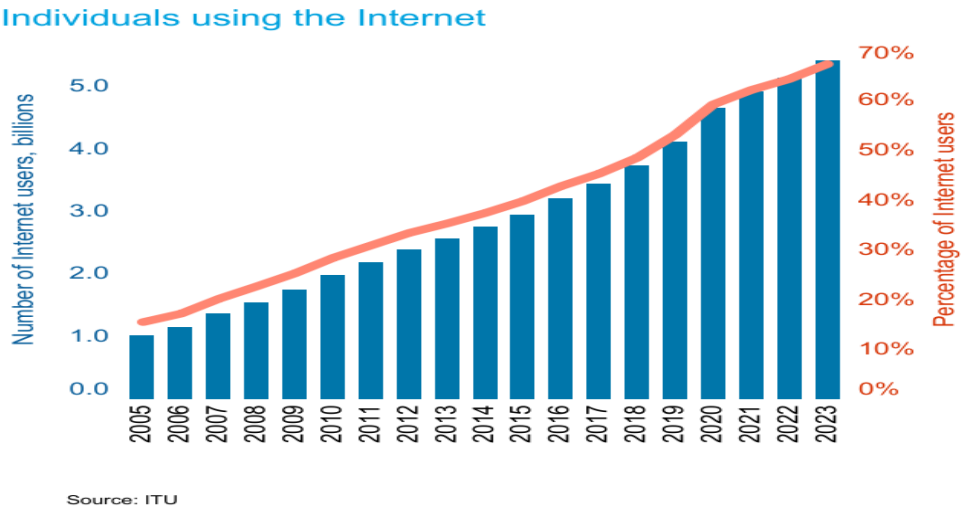
Kibermakon, birinchi navbatda, kompyuterlar va kompyuter xotirasi orqali dunyoda ishlatiladigan ochiq maydon tushunchasini anglatadi. Ilk bor kibermakon

atamasi 1986-yilda Uilyam Gibsonning «Burning Chrome»[1] romanida qo‘llangan. Shuningdek, fransuz faylasufi Per Levining fikricha, kiberfazo silliq, yuqori aniqlangan, interaktiv va real vaqt rejimida ishlov berish maydonidir[2]. Bu makon axborotni olish, uzatish, modellashtirish va ro‘yxatga olish imkonini beradi[3]. Xitoylik strateg va mutafakkir Sun Tszi o‘zining «Urush san’ati» risolasida qurolsiz kurashish va jangsiz g‘alaba qozonish kerakligini donolik bilan ta’kidlagan[4]. Bir ming yildan ko‘proq vaqt o‘tdi, ammo g‘oya o‘z dolzarbligini yo‘qotmadi. 21-asrda davlatlar odatiy qurollar o‘rniga axborot resurslaridan foydalanishga harakat qilmoqdalar.

Aytishimiz mumkinki, kiber urushlar olib borilmoqda. Kiberxavfsizlikni ta’minlash muammosi bugungi kunda ilg‘or axborot texnologiyalariga ega har bir davlat duch keladigan global muammodir. Xitoy Xalq Respublikasi axborot xavfsizligini ta’minlash masalasiga g‘arbdan sezilarli darajada farq qiluvchi o‘ziga xos xususiyatlar bilan yondashadi. Davlat uchun muhim bo‘lgan ma’lumotlarning chiqib ketishi yoki kiruvchi ma’lumotlar kirib kelishining oldini olish maqsadida Xitoy ba’zi ijtimoiy tarmoqlar va qidiruv tizimlarini bloklashni afzal ko‘radi. Xitoyning terminologiyaga munosabati ham boshqacha: ular zararli axborot tarqalishining oldini olishni nazarda tutuvchi «kiberxavfsizlik» tushunchasidan ko‘ra «axborot xavfsizligi»ni afzal ko‘radi. Kiberxavfsizlik masalasidagi bunday qarama-qarshiliklar Pekinning g‘arb davlatlari bilan muloqotini murakkablashtiradi[5].

Xalqaro elektraloqa ittifoqining[6] (XEI) internet tarmoqlarida bergan hisobotiga ko‘ra, dunyo aholisining yarmi internetdan foydalanadi. Rivojlangan mamlakatlarda onlayn aholi umumiy aholining 80 foizdan ortig‘ini tashkil qiladi. Biroq, shu bilan birga, rivojlanayotgan mamlakatlarda onlayn foydalanuvchilar soni doimiy ravishda ortib bormoqda. Agar 2005 yilda bu ko‘rsatkich 7,7 foizni tashkil etgan bo‘lsa, hozir bu ko‘rsatkich 43,5 foizni tashkil etmoqda. XEI ma’lumotlariga ko‘ra, Afrika mintaqasi eng yuqori o‘sishga ega. Afrikada 2005-yilda aholining 2 foizi internetdan foydalangan bo‘lsa, 2018-yilda bu ko‘rsatkich 25 foizni tashkil qilgan[7]. Hisobotda aytilishicha, eng past o‘sish Yevropa va Amerikada kuzatilgan. Osiyo-Tinch okeani havzasi eng past foydalanish stavkalariga ega.

[1] Gibson, William, Burning chrome. - USA.: New York: Arbor House, 1986. - 220 p.
[2] Lévy P., World Philosophie: le marché, le cyberespace, la conscience, Odile Jacob, Paris 2000. 224 p.
[3] https://project7155832.tilda.ws/.
[4] Сунь Цзы. Искусство войны. - М.: София, 2010. - С. 56-58.
[5] Сейранова С.Н. Киберугрозы как серьезный вызов национальной безопасности КНР / С.Н. Сейранова// Актуальные проблемы современных международных отношений. - 2017. - С. 131-136.
[6] https://www.itu.int/ru/Pages/default.aspx.
[7] https://en.wikipedia.org/wiki/Internet_in_Africa.



Xalqaro elektraloqa ittifoqining 2023-yilda taxminan 5,4 milliard odam yoki dunyo aholisining 67 foizi internetdan foydalanadi. Bu 2018-yilga nisbatan 45 foizga ko‘proqdir, bu davrda taxminan 1,7 milliard kishi internetga ulangan. Biroq, natijada 2,6 milliard odam hali internetga ulanmagan[8].

Kiberxavfsizlik - bu tizimlar, tarmoqlar va dasturiy ta’minotni raqamli hujumlardan himoya qilish bo‘yicha chora-tadbirlarni amalga oshirishdir[9]. Bunday hujumlar odatda maxfiy ma’lumotlarga kirish, uni o‘zgartirish, yo‘q qilish, foydalanuvchilardan mablag‘ olish, tashkilotlar yoki kompaniyalarning normal faoliyatini buzish maqsadida amalga oshiriladi. «Zamonaviy dunyoda kibertahdidlar soni tez sur’atlar bilan o‘sib bormoqda.

Jahon ommaviy axborot vositalarining yangiliklar lentalari har kuni yangi voqealar haqida xabar beradi. Korxonalar va davlat idoralari hujumlar to‘lqiniga dosh berishga harakat qilmoqda, xakerlar oddiy fuqarolarning bank hisoblarini bo‘shatishmoqda va shuning uchun raqamli dunyoda tahdidlardan ishonchli himoya qilish asosiy ehtiyojga aylanmoqda»[10].

«Kiberjinoyatchilik» tushunchasi axborot-kommunikatsiya texnologiyalari vositalaridan foydalangan holda, virtual tarmoqda dahshat solish, virus va boshqa zararli dasturlar, qonunga zid axborotlar tayyorlash va tarqatish, elektron xatlarni ommaviy tarqatish (spam), xakerlik hujumi, veb-saytlarga noqonuniy kirish,

[8] Committed to connecting the world https://www.itu.int/en/ITUD/Statistics/Pages/stat/default.aspx.
[9] Кибертерроризм - новые угрозы и предпосылки терроризма: проблемы, пути решения: сборник научных статей / Министерство науки и высшего образования РФ, Алтайский государственный университет, Юридический институт, Региональный антитеррористический научно-методический центр, Кафедра уголовного права и криминологии; редакторы: Валерий Анатольевич Мазуров, Мария Александровна Стародубцева. – Барнаул.: Алтайского государсвенного. университета, 2021. - 168 с.
[10] https://www.ptsecurity.com/ru-ru/research/knowledge-base/chto-takoe-kiberbezopasnost.

firibgarlik, ma’lumotlar butunligi va mualliflik huquqini buzish, kredit kartochkalari raqami hamda bank rekvizitlarini o‘g‘irlash (fishing va farming) va boshqa turli huquqbuzarliklar bilan izohlanadi»[11]. Kibermakon xavfining muhim ko‘rsatkichi - bu juda katta hajmdagi ma’lumotlarga kirish. Internetdagi ma’lumotlar ko‘pincha davlat va nodavlat tuzilmalar tomonidan har qanday g‘oyalarni ilgari surish uchun ishlatiladi. Internetdan bunday jinoiy foydalanishning yorqin misoli «Islomiy davlat» radikal tashkiloti tomonidan yangi terrorchi agentlarni onlayn yollashdir[12].

Kiberterrorizm - terroristik maqsadlar yo‘lida kompyuter va telekommunikatsiya texnologiyalari (asosan internet)dan foydalanish. Kiberterrorizm, shuningdek, maxsus xaker dasturlari orqali kompyuter boshqaruvi tarmoqlarini egallab olish va kompyuter viruslari yordamida internet tarmog‘ida terakt sodir etish, internet tarmog‘ini ishdan chiqarishni ko‘zda tutadi[13]. Har bir tashkilot davom etayotgan yoki muvaffaqiyatli hujumlarga qarshi bir qator asosiy choralarni ko‘rishi kerak. Ishonchli harakatlar rejasi yagona markazdan boshqarilishi kerak. Ushbu keng qamrovli chora-tadbirlar hujumlarni qanday aniqlash, tizimlarni himoya qilish, tahdidlarni aniqlash, ularni yo‘q qilish va hujumlardan keyin operatsiyalarni tiklashni tushuntirishi kerak. Texnologiyalar tashkilotlar va individual foydalanuvchilarni kiberhujumlardan himoya qilish uchun zarur vositalar bilan ta’minlashda muhim element hisoblanadi. Himoya qilinishi kerak bo‘lgan asosiy komponentlar - bu: kompyuterlar;, aqlli qurilmalar;, marshrutizatorlar;, modemlar, tarmoqlar;, bulutli muhit.

Yuqoridagi ro‘yxatdagi komponentlarni himoya qilish uchun ishlatiladigan eng keng tarqalgan texnologiyalar qatoriga yangi avlod tarmoqli: routerlarini amalga oshirish;, DNS filtrlash;, zararli dasturlardan himoya qilish;, virusga qarshi dasturlarni yuklab olish; elektron pochtani himoya qilishlar kiradi.

Zamonaviy dunyoda ilg‘or kiber himoya dasturlari har bir foydalanuvchining manfaatlarini himoya qiladi. Individual darajada, kibermudofaa hujumi shaxsiy ma’lumotlarning o‘g‘irlanishi, pul mablag‘lari yoki oilaviy fotosuratlar kabi qimmatli ma’lumotlarning yo‘qolishi, keng miqyosda davlat va harbiy sirlarni oshkor qilish kabi salbiy oqibatlarga olib kelishi mumkin. Elektr stansiyalari, shifoxonalar, moliyaviy xizmatlar ko‘rsatuvchi bank sektori va boshqa institutlar kabi barcha muhim infratuzilmalarni himoya qilish jamiyatimiz hayoti va faoliyatini ta’minlash uchun juda muhimdir[14].

[11] https://iiv.uz/oz/news/kiberjinoyatchilikka-qarshi-kiberxavfsizlik.

[12] Смирнова А.А., Захарова Т.Ю., Синогина Е.С. Киберугрозы безопасности подростков // Научно педагогическое обозрение (Pedagogical Review). - 2017. Вып. 3 (17). С. 99-107.

[13] Кибертерроризм как новая разновидность терроризма. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3927791

[14] В.С.Овчинский. Основы борьбы с киберпреступностью и кибертерроризмом хрестоматия / составитель заслуженный юрист Российской Федерации, Докт. юридич. наук. - М.: Норма, 2017. - 527 с.

1977-yildagi AQSh fiskal daromadining qariyb yarmi shu sektordan olingan. Shu sababli, bu yangi tug‘ilgan ijtimoiy tuzilishga turli nomlar berilgan. Masalan, Masuda va Porat uni «Axborotlashgan jamiyat»[15] deb nomlagan. Axborotlashgan jamiyat turlicha yondashuvlarga ega. Eng avvalo, axborotlashgan jamiyat bu so‘nggi davrda o‘z izini qoldirgan axborot portlashi natijasida asosiy ishlab chiqarish omili axborot bo‘lgan va axborotni qayta ishlash va saqlashda kompyuter va kommunikatsiya texnologiyalariga asoslangan ijtimoiy tuzilmadir. Bundan tashqari, mamlakatdagi axborotlashgan jamiyatni baholashda ushbu mamlakat YAIMning necha foizi bevosita yoki bilvosita axborot sohasiga bog‘liqligiga qarab amalga oshirilishi mumkin.

Axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi kiberjinoyatlarning paydo bo‘lishiga va uning kundan-kunga ortib borishiga olib keldi. Birlashgan Millatlar Tashkiloti hisobotida aytilishicha, har yili 1,5 milliondan ortiq odam kiberjinoyat qurboni bo‘ladi va kiberjinoyatlarning umumiy qiymati 1 milliard dollardan oshadi[16].

Kiberjinoyatlarning ko‘payishi davlat boshqaruvi, bank, transport, milliy xavfsizlik va boshqa tizimlarni takomillashtirish va butun dunyo bo‘ylab kibermudofaa choralarini kengaytirishni dolzarb qiladi. 2012-yilda AQShning Chikago shahrida bo‘lib o‘tgan NATO sammitida qabul qilingan yakuniy ma’qullashda kiberhujumlar soni va sifati oshishi faktlari yana bir bor tilga olindi va alyansga a’zo davlatlar hamda xalqaro tashkilotlar bilan (BMT, Yevropa Ittifoqi, Yevropa Kengashi va boshqalar) yagona kibermudofaa tashkil etish muhimligi ta’kidlandi.

AQSh, Rossiya, Xitoy, Angliya, Fransiya, Germaniya va boshqa bir qator rivojlangan davlatlar allaqachon o‘zlarining maxsus kiberqo‘shinlarini yaratgan. Garchi bu davlatlar o‘zlarining asosiy maqsadi o‘z tarmoqlarini himoya qilish ekanligini ta’kidlagan bo‘lsalar-da, bu yerda hujum operatsiyalari ham ko‘zda tutilgan. Ko‘p yillar davomida Qo‘shma Shtatlar va Rossiya saylovoldi kampaniyalarida amaldagi prezidentlarga, hatto ularning eng yaqin ittifoqchilariga qarshi keng ko‘lamli elektron josuslik amaliyotlarini o‘tkazgani haqida keng ko‘lamli dalillar mavjud. Yaqinda AQSh va Meksikada bo‘lib o‘tgan saylovlar global axborot tarmog‘i, internetni global jang maydoniga aylantirdi.

[15] Йонеджи Масуда. «Общество информации как постиндустриальное», Рио/Embratel, Рио-де-Жанейро, 1980.; Порат, Марк Ури (май 1977). Информационная экономика: определение и измерение. Вашингтон, Округ Колумбия: Министерство торговли Соединенных Штатов. OCLC 5184933.

[16] https://cyberleninka.ru/article/n/kiberprestupnost-kak-tenevoy-biznes.; https://www.un.org/ru/desa/cybersecurity-demands-global-approach.

AQSh Milliy xavfsizlik agentligining maxfiy hujjatlaridan birida navbatdagi yirik keng ko‘lamli mojaro kibermakonda boshlanishi haqida ma’lumot bor. AQSh haqiqatda kiber urush boshlagan yagona davlatdir. Hech kimga sir emaski, AQShning sobiq prezidenti Obama Eronning minglab yadro sentrifugalarini yo‘q qilish uchun kiberhujumga buyruq bergan. Kompyuter viruslari bilan amalga oshirilgan kuchli texnologik hujum natijasida amerikalik xakerlar Eronga katta moddiy zarar yetkazgan holda yadroviy dasturni ikki yilga orqaga qaytarishga muvaffaq bo‘lishdi. Endi hech kim bu tezkor ma’lumotlarni, ya’ni «kiber kuchlar» amaliyotini avvalgidek qunt bilan yashirishga urinmayapti[17].

Dunyo bo‘ylab ko‘plab armiyalar allaqachon kiberhujumlarga qarshi amaliy jangovar mashqlarni o‘zlarining jangovar tayyorgarlik dasturlariga kiritmoqda. 2008-yilda tashkil etilgan NATOning Kibertahdidlarga qarshi kurash markazi (CCDCOYE) tomonidan o‘tgan 2023-yili tashkil etilgan mashg‘ulotlar davomida ishtirokchilar hatto «harakatlanuvchi o‘q poyezdini to‘xtatishga harakat qilishgan». Stajjor bo‘lgan xakerlar guruhi muvaffaqiyatga erishdi: ular poyezdni to‘xtatib, boshqaruv tizimini buzib, dvigatelni to‘sib qo‘yishga muvaffaq bo‘lishdi. Ushbu treninglarda qatnashadigan xakerlar faqat taklifnoma bilan kiritiladi[18].

Dunyoning bir bo‘lagi bo‘lgan O‘zbekistonda zamonaviy axborot-kommunikatsiya texnologiyalarini (AKT) keng tatbiq etishda ushbu sohada uzluksiz kiberxavfsizlik choralarini amalga oshirishga jiddiy e’tibor qaratilmoqda. Turli davrlarda kiber va axborot xavfsizligi masalalariga bag‘ishlangan xalqaro tadbirlarda ishtirok etgan O‘zbekiston Respublikasining rasmiy pozitsiyasi ushbu sohani rivojlantirishga alohida e’tibor qaratish va uni ustuvor yo‘nalish deb e’lon qilishdan iborat bo‘ldi. Toshkent Yevropa Kengashi, Yevropa Ittifoqi, NATO, Xalqaro elektr aloqa ittifoqi va boshqa xalqaro tashkilotlar bilan kiberxavfsizlik va axborot xavfsizligi masalalarida faol aloqalarni davom ettirmoqda. Bu sohada huquqiy bazani shakllantirish maqsadida O‘zbekiston xalqaro konvensiya va dasturlarga qo‘shildi, shuningdek, ichki qonunchilik bazasini takomillashtirdi.

Respublikada axborot jarayonlarini muhofaza qilish, barqarorligi va uzluksizligini ta’minlash, davlat organlarining axborot resurslarini muhofaza qilish, ushbu sohadagi tahdidlarning oldini olish, tahlil qilish, baholash bo‘yicha davlat va nodavlat axborot infratuzilmasi subektlari hamda ulardan foydalanuvchilarning faoliyatini muvofiqlashtirish va kiberxavfsizlik sohasida xatarlarni boshqarish, umummilliy tayyorgarlik va ogohlantirish maqsadida O‘zbekiston Respublikasi

[17] Клебанов Л.Р., Полубинская С.В. Компьютерные технологии в совершении преступлений диверционной и террористической направленности // Вестник Российского университета дружбы народов. Серия: Юридические науки. 2020. Т. 24. № 3. С. 717-734.
[18] https://ccdcoe.org/.

Prezidentining 2023-yil 31-maydagi PQ-167-son «O‘zbekiston Respublikasining muhim axborot infratuzilmasi obektlari kiberxavfsizligini ta’minlash tizimini takomillashtirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida»gi [19] Qarori imzolangan. «Kiberxavfsizlik markazi» DUKning AKT Sertifikatlashtirish organi tomonidan «Updive SIEM» dasturiy ta’minoti bo‘yicha sertifikatlashtirish sinov ishlari muvaffaqiyatli yakunlandi. 2023-yilning 19-oktabrda «Updive SIEM» xavfsizlik ma’lumotlari va xavfsizlik hodisalarini boshqarish tizimining dasturiy ta’minoti uchun kiberxavfsizlik talablari asosida muvofiqlik sertifikati rasmiylashtirildi. Mazkur tizim O‘zbekiston Respublikasi «UPDIVE» MCHJning dasturchilari tomonidan ishlab chiqilgan bo‘lib, Adliya vazirligidan «Updive SIEM» dasturiy ta’minoti intellektual mulk obekti sifatida rasmiy ro‘yxatdan o‘tkazilganligi to‘g‘risidagi Guvohnomaga ega»[20].

Bugungi kunda kiberxavfsizlik, onlayn xavfsizlik, tarmoqlar ishonchliligi uchun hal qiluvchi xavfsizlik masalalari eng muhim ustuvor yo‘nalishlardan biri sifatida qaralmoqda. Samarali xalqaro hamkorlik, ko‘p tomonlama muloqotga erishish, ushbu qarorlarni muvaffaqiyatli qabul qilish va amalga oshirish maqsadida davlat, nodavlat va xalqaro tashkilotlar tomonidan har yili mintaqaviy va jahon miqyosida turli darajadagi tadbirlar o‘tkazilmoqda. Bu, o‘z navbatida, davlatimiz tomonidan ushbu sohada amalga oshirilayotgan siyosatni xalqaro maydonda ham davom ettirish, eng so‘nggi yangiliklarni o‘rganish, fikr va tajriba almashish uchun umumiy bazani tashkil etish uchun keng imkoniyatlar yaratish imkonini bermoqda. Ko‘rinib turibdiki, kiberxavfsizlik juda keng, dolzarb muammo bo‘lib, O‘zbekiston davlati bu sohadagi mavjud bo‘shliq va tahdidlarni baholab, tegishli choralarni ko‘rmoqda. Olimlarning fikriga ko‘ra, kompyuterlashtirishning jadal o‘sishi kibertahdidlarning tobora ortib borishi bilan birga keladi, bu esa bolalar va yoshlarning manfaatlariga katta darajada ta’sir qiladigan kiberjinoyatchilikning yangi shakllarini keltirib chiqaradi (bu empirik psixodiagnostik tadqiqotlar bilan tasdiqlangan). Shu munosabat bilan «yoshlarning kiber qurbonligining sabablarini o‘rganish, kiberqurbonlarning individual shaxsiy xususiyatlarini o‘rganish, kibermakon foydalanuvchilarida kiberqurbonlik xulq-atvorini shakllantirishning psixologik mexanizmlari, qidiruv tizimini yangilash taklif etilmoqda. Yoshlar muhiti vakillarining kiberxavfsizligini ta’minlash» [21] muhim hisoblanadi. «Mamlakatimizda olib borilayotgan islohotlar zamirida xalq farovonligi yotar ekan, xalq farovonligini ta’minlash, aholining davlat organlariga bo‘lgan

[19] O‘zbekiston Respublikasi Prezidentining 2023-yil 31-maydagi PQ-167-son «O‘zbekiston Respublikasining muhim axborot infratuzilmasi obyektlari kiberxavfsizligini ta’minlash tizimini takomillashtirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida»gi Qarori/ Qonunchilik ma’lumotlari milliy bazasi, 02.06.2023 y., 07/23/167/0321-son
[20] https://csec.uz/uz/news/mahalliy-yangiliklar/yurtimizda-mahalliy-siem-tizimining-dasturiy-taminoti-sertifikatlan di/.
[21] Чусавитина Г.Н., Зеркина Н.Н. Профилактика киберэкстремизма в системе современной высшей школы как социальная проблема // Мир науки. Социология, филология, культурология. 2016. № 1. С. 2.

ishonchini yanada oshirish, olib borilayotgan islohotlarni yanada takomillashtirish va yaratilayotgan kiberxavfsizlikni ta’minlash maqsadida kiberjinoyatchilik bo‘yicha islohotlarni yangi bosqichga ko‘tarish maqsadga muvofiqdir»[22]. «Bugungi kunda mamlakatimizda sog‘lom internet-muhitiga ega axborotlashgan jamiyatni rivojlantirish, milliy saytlarni ko‘paytirishga alohida e’tibor qaratilmoqda. Internetda milliy veb-saytlarni yaratishga qaratilgan ko‘rik-tanlovlarning o‘tkazilayotgani, veb-ixtirochilarning moddiy va ma’naviy jihatdan qo‘llab-quvvatlanayotgani, sog‘lom axborot muhitini tarkib toptirishga yo‘naltirilgan turli tadbirlar ana shu maqsadga xizmat qilmoqda. Shu bilan bir qatorda, shaxslarni internet hamlalaridan himoyalash, axborot olish va tarqatish madaniyatining targ‘ib qilish, tarmoq xavfsizligini ta’minlash yuzasidan chora-tadbirlar amalga oshirilmoqda. Ommaviy axborot vositalari orqali muntazam ravishda internet tarmoqlaridan foydalanish qoidalari, veb-makondagi xavf va firibgarliklarga qarshi kurashish usullari tushuntirilmoqda»[23].

Kiberhujum zamonaviy davrning asosiy tahdidlaridan biridir. Kibermakondagi tahdidlar yangi hodisa emas. Zamonaviy kibermakon milliy xavfsizlik nuqtai nazaridan mudofaa tizimini yaratishni talab qiladi. Chunki kompyuterlar va internet texnologiyalari ko‘plab muhim sohalarni boshqarish va ulardan foydalanishda keng qo‘llaniladi. Shuningdek, har qanday vaqtda kiberhujumlar natijasida o‘sha tizimlarning ishdan chiqishiga olib kelishi mumkin. (Xakerlar “Hacker” inglizcha so‘z bo‘lib, hack buzib tashlamoq, sindirmoq degan ma’nolarni bildiradi)[24]. Ilk davrlarda xaker deganda ko‘proq dasturlash bilan yuqori saviyada shug‘ullanuvchi shaxs tushunilar edi. Ammo yillar o‘tgan sayin xaker so‘zi ko‘proq kompyuterlar bo‘yicha o‘zining keng bilimlarini noqonuniy va zararli faoliyat uchun ishlatadigan jinoyatchi sifatida tushuniladi.

Shu o‘rinda tarixga nazar tashlasak, xakerlar birinchi marta o‘tgan asrning 60-yillarida Massachusets shtat texnologiya institutining sun’iy intellekt laboratoriyalarida paydo bo‘lgan. 70-yillarda keng tarqalgan telefon tizimlariga ruxsatsiz kirish 80-yillarda kompyuter sohasida o‘zini namoyon qila boshladi.

80-yillarda kompyuterlarda elektron nashriyot tizimi - BBS ishlatilgan. 80-yillarda xakerlik guruhlari rivojlana boshladi va AQShda «Legion of Doom»[25], Germaniyada «Chaos Compyuter Club»[26] kabi guruhlar paydo bo‘ldi. Hukumat va

[22] А.У.Анорбоев Кибержиноятчилик, унга қарши курашиш муаммолари ва киберхавфсизликни таъминлаш истиқболлари. - Тошкент.: 2020. - 197 б.
[23] Қосимов Ш. (2022). Интернет тармоқлари орқали содир этилаётган жиноятларни фош этишни такомиллаштиришнинг айрим муаоммолари. Евразийский журнал права, финансов и прикладных наук, 2 (9), 16-23. извлечено от https://in-academy.uz
[24] https://en.wikipedia.org/wiki/Hacker.
[25] https://en.wikipedia.org/wiki/Legion_of_Doom.
[26] https://ru.wikipedia.org/wiki/Chaos_Computer_Club.

kompaniyalar kompyuterlariga ruxsatsiz kirishning kuchayishi AQSh Kongressini aniq choralar ko‘rishga majbur qildi[27]. Natijada Kongress xakerlikni jinoyat deb hisoblovchi qonun qabul qildi. Biroq, qonun muayyan yoshga to‘lmaganlarga nisbatan qo‘llanilmadi.

Kornel universitetining Milliy xavfsizlik byurosida ishlagan Robert Morris ismli talaba hukumatga qarashli ARPANET ma’lumotlar tarmog‘iga (hozirgi internetning «otasi») o‘zini ko‘paytiruvchi virusni joylashtirgan. Virus 6000 ta kompyuterdan iborat ma’lumotlar tarmog‘ida tez tarqalib, hukumat va universitet kompyuterlariga kirishni bloklab qo‘ygan. 1988-yilda Robert Morris internetga joylagan virus ko‘plab kompyuterlarni yaroqsiz holga keltirdi. Robert Morris Kornel universitetidan haydalgan, uch yil sinov muddatiga o‘tgan va 10 ming dollar jarimaga tortilgan[28]. 1990-yilda uzoq davom etgan tergovdan so‘ng AQSh maxsus xizmatlari 14 ta shaharda yirik «xakerlik operatsiyasi»[29]ni boshladi. Operatsiyada kompyuter, kredit karta va telefon bilan firibgarlik qilgan juda ko‘p odam qo‘lga olindi. Bu operatsiya xakerlik guruhlariga katta zarba berdi. Shu bilan birga, xakerlarning amnistiya uchun bir-birlarini oldi-sotdi qilishlari ular o‘rtasida bo‘linishga olib keldi. Bu operatsiya tarixda «Sundevil operatsiyasi»[30] nomi bilan qoldi.

1990-yillarda AQShning Markaziy razvedka boshqarmasi, NASA va Pentagon kabi muhim tashkilotlarining kompyuter tizimlari yoki veb-saytlari bir necha bor buzib kirilgan. O‘sha yillarda 30 yoshda bo‘lgan Devid Smit Las-Vegasdagi sevgilisi Melissa nomidagi virus bilan o‘zini butun dunyoga tanitdi. 300 ta jahon miqyosidagi kompaniya ma’lumotlarining to‘liq o‘chirilishiga olib kelgan ushbu virus jami 400 million dollar zarar keltirdi. Qo‘lga olingan Smit besh yillik qamoq jazosiga hukm qilindi. Windows 98 operatsion tizimi chiqarilgandan so‘ng, 1999-yil «xavfsizlik va xakerlik yili»[31] bo‘ldi. Operatsion tizimda ko‘p sonli xavfsizlik muammolari paydo bo‘ldi va kompyuterlarni xakerlardan himoya qiluvchi mahsulotlar bozori paydo bo‘ldi.

Zamonaviy axborot jamiyatida ommaviy axborot vositalarining o‘rni va roli juda katta. Globallashuv har bir milliy davlatga jamiyatning yangi modelini taqdim etadi va milliy jamiyatlarda bu modelni o‘zgartirish yoki ba’zan rad etishdan boshqa iloji yo‘q. Shunday ekan, jamiyatning qabul qilingan yangi turi biz axborot jamiyati sifatida tavsiflaydigan ijtimoiy tabaqalanishni shakllantiradi. Axborot jamiyatining

[27] https://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act.
[28] https://en.wikipedia.org/wiki/Morris_worm#:~:text=The%20Morris%20worm%20or%20Internet,Computer%20Fraud%20and%20Abuse%20Act.;https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218.
[29] https://en.wikipedia.org/wiki/Operation_Sundevil.
[30]https://sushiandbox.ru/uz/socialnye-seti/istoriya-hakinga-hakery.
[31] https://edition.cnn.com/2001/TECH/internet/11/19/hack.history.idg/?related.

an’anaviy milliy-madaniy yoki diniy-madaniy jamiyatlardan farqi shundaki, axborot jamiyati milliy-axloqiy qadriyatlar, an’analar, milliy mentalitetga emas, balki jamiyat tomonidan iste’mol qilinadigan axborotga asoslanadi. Jamiyatning axborot makonida mavjud bo‘lgan axborot almashinuvi, ishlab chiqarilishi va iste’mol qilinishi, aslida, yangi jamiyatning shaxsi bo‘lgan odamlarning tafakkurini, turmush tarzini, voqealarga qarashini, ularning xatti-harakatlarini belgilaydi. Ushbu xatti-harakatlarning shakli axborot makonida aylanib yuradigan ma’lumotlarning sifatiga bog‘liq. Binobarin, har bir milliy davlatning axborot makonini bashorat qilish va milliy manfaatlar nuqtai nazaridan maqsadli shakllantirish, uni nazorat qilish va yo‘naltirish zarur.

Ko‘p hollarda ommaviy axborot vositalarining funksiyasi haqida gapirganda, uning birinchi vazifasi - bu ommaviy axborot vositalarining jamiyatni axborot bilan ta’minlash vazifasini esga olamiz. Biroq hozirgi sharoitda zamonaviy axborot jamiyatlarida ommaviy axborot vositalarining funksiyasi ham, jamiyatning ommaviy axborot vositalariga munosabati ham bu bilan cheklanmaydi. Chunki zamonaviy bosqichda ommaviy axborot vositalari, jamiyat, davlat munosabatlari shunday darajaga yetdiki, bu munosabatlar millat va xalq, milliy davlat taqdiri nuqtai nazaridan juda muhim vositaga aylandi. Shuning uchun bu munosabatlar tizimida axborot nafaqat axborot, balki boshqaruvni amalga oshiruvchi funksional birlik vazifasini ham bajaradi. Bunday holda, biz allaqachon ma’lumotni maxsus maqsadli institusional vosita sifatida ko‘rib chiqishimiz mumkin. Demak, axborotning sifati va ta’sir doirasidagi oqibatlari yoki milliy manfaatlar nuqtai nazaridan olib kelishi mumkin bo‘lgan dividendlar juda ko‘p.

Shu ma’noda O‘zbekiston uchun axborot makonini himoya qilish, undan axborot xavfsizligi, milliy va davlat manfaatlarini ta’minlashda foydalanish nihoyatda muhimdir. Bugun O‘zbekistonning axborot makonida nafaqat bosma ommaviy axborot va klassik ommaviy axborot vositalari, balki internet va ijtimoiy tarmoqlar ham o‘z ichiga olganini inobatga olsak, axborotning ahamiyati naqadar oshganiga yana bir bor guvoh bo‘lamiz. Shuningdek, bugungi kunda axborotni boshqaruvchi, uni ishlab chiqaruvchi, uzatuvchi, axborot tashuvchisi bo‘lgan yoki axborot manbai vazifasini bajaruvchi shaxslar ko‘p bo‘lsa, kiber yoki axborot makonini boshqarish va yo‘nalishi dolzarb vazifalardan biriga aylanadi.

XULOSA VA TAKLIFLAR (CONCLUSION/RECOMMENDATIONS). Kibertahdid - bu raqamli muhitda xavfsizlik va barqarorlikka putur yetkazuvchi hodisa yoki jarayonlar majmuasidir. Ular odatda kompyuter tarmoqlari, internet va texnologiyalar orqali amalga oshiriladi. Kibertahdidlarning ma’naviy-axloqiy tarbiya bilan bog‘liqligi asosan kiberfazoda yuzaga keladigan xatti-harakatlar, insonlararo

muloqot va ta’sir jarayonlari bilan uzviy bog‘liqdir. Yoshlar kibermuhitda ko‘pincha turli tahdidlar, axloqiy me’yorlardan chetga chiqish yoki zararli axborot bilan yuzma-yuz bo‘lishadi. Shu nuqtai nazardan, ma’naviy-axloqiy tarbiya kibertahdidlarni anglash va ularga qarshi turishda muhim vosita hisoblanadi.

Ijtimoiy tarmoqlarda yoki boshqa onlayn platformalarda zo‘ravonlik va tahqirlash ma’naviy-axloqiy me’yorlarga zid keladi. Yoshlarning ruhiy salomatligi va axloqiy qadriyatlarini buzadigan bu holatlar ularga jiddiy zarar yetkazishi mumkin. Ma’naviy tarbiya kibermadaniyatni shakllantirish, to‘g‘ri kommunikatsiyani o‘rgatish va inson huquqlarini himoya qilish orqali bunday tahdidlarni kamaytirishda muhim rol o‘ynaydi. Onlayn axborot oqimida tez-tez uchraydigan bu tahdid turli noto‘g‘ri va axloqiy me’yorlarga zid axborotlarni tarqatish orqali jamiyatda ijtimoiy nizolarni keltirib chiqaradi. Yoshlar ma’naviy tarbiyani mustahkam olgan taqdirda, axborotlarni tahlil qilish va to‘g‘ri manbalardan foydalanish ko‘nikmalariga ega bo‘lishadi.

Xulosa qilib aytganda, kibertexnologiyalar va raqamli vositalarning jamiyat hayotidagi o‘rni, ayniqsa, ma’naviy-axloqiy tarbiya sohasida tobora ortib bormoqda. Shu bilan birga, bu jarayonlarda axloqiy mas’uliyat va ma’naviy qadriyatlarning ahamiyati yanada dolzarb bo‘lmoqda.

FOYDALANGAN ADABIYOTLAR:

1. Gibson, William, Burning chrome. - USA.: New York: Arbor House, 1986. - 220 p.
2. Lévy P., World Philosophie: le marché, le cyberespace, la conscience, Odile Jacob, Paris 2000. 224 p.
3. Сунь Цзы. Искусство войны. - М.: София, 2010. - С. 56-58.
4. Сейранова С.Н. Киберугрозы как серьезный вызов национальной безопасности КНР / С.Н. Сейранова// Актуальные проблемы современных международных отношений. - 2017. - С. 131-136.
5. Кибертерроризм - новые угрозы и предпосылки терроризма: проблемы, пути решения: сборник научных статей / Министерство науки и высшего образования РФ, Алтайский государственный университет, Юридический институт, Региональный антитеррористический научно-методический центр, Кафедра уголовного права и криминологии; редакторы: Валерий Анатольевич Мазуров, Мария Александровна Стародубцева. – Барнаул.: Алтайского государсвенного. университета, 2021. - 168 с.
6. Смирнова А.А., Захарова Т.Ю., Синогина Е.С. Киберугрозы безопасности подростков // Научно педагогическое обозрение (Pedagogical Review). - 2017. Вып. 3 (17). С. 99-107.

7. В.С.Овчинский. Основы борьбы с киберпреступностью и кибертерроризмом хрестоматия / составитель заслуженный юрист Российской Федерации, Докт. юридич. наук. - М.: Норма, 2017. - 527 с.
8. Йонеджи Масуда. «Общество информации как постиндустриальное», Рио/Embratel, Рио-де-Жанейро, 1980.;
9. Порат, Марк Ури (май 1977). Информационная экономика: определение и измерение. Вашингтон, Округ Колумбия: Министерство торговли Соединенных Штатов. OCLC 5184933.
10. Клебанов Л.Р., Полубинская С.В. Компьютерные технологии в совершении преступлений диверсионной и террористической направленности // Вестник Российского университета дружбы народов. Серия: Юридические науки. 2020. Т. 24. № 3. С. 717-734.
11. O‘zbekiston Respublikasi Prezidentining 2023-yil 31-maydagi PQ-167-son «O‘zbekiston Respublikasining muhim axborot infratuzilmasi obyektlari kiberxavfsizligini ta’minlash tizimini takomillashtirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida»gi Qarori/ Qonunchilik ma’lumotlari milliy bazasi, 02.06.2023 y., 07/23/167/0321-son
12. Чусавитина Г.Н., Зеркина Н.Н. Профилактика киберэкстремизма в системе современной высшей школы как социальная проблема // Мир науки. Социология, филология, культурология. 2016. № 1. С. 2.
13. А.У.Анорбоев Кибержиноятчилик, унга қарши курашиш муаммолари ва киберхавфсизликни таъминлаш истиқболлари. - Тошкент.: 2020. - 197 б.
14. Қосимов Ш. (2022). Интернет тармоқлари орқали содир этилаётган жиноятларни фош этишни такомиллаштиришнинг айрим муаоммолари. Евразийский журнал права, финансов и прикладных наук, 2 (9), 16-23. извлечено от https://in-academy.uz
15. https://en.wikipedia.org/wiki/Hacker.
16. https://en.wikipedia.org/wiki/Legion_of_Doom.
17. https://ru.wikipedia.org/wiki/Chaos_Computer_Club.
18. https://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act.
19. https://en.wikipedia.org/wiki/Morris
20. https://en.wikipedia.org/wiki/Operation_Sundevil.
21. https://sushiandbox.ru/uz/socialnye-seti/istoriya-hakinga-hakery.
22. https://edition.cn.com/2001/TECH/internet/11/19/hack.history.idg/?related.
23. https://www.itu.int/ru/Pages/default.aspx.
24. https://en.wikipedia.org/wiki/Internet_in_Africa.

25. Committed to connecting the world https: //www. itu.int/ en/ITUD /Statistics /Pages/stat/default.aspx.
26. https://www.ptsecurity.com/ru-ru/research/knowledge-base/chto-takoe-kiberbezopasnost.
27. https://iiv.uz/oz/news/kiberjinoyatchilikka-qarshi-kiberxavfsizlik.
28. Кибертерроризм как новая разновидность терроризма. https://papers.ssrn.com/sol3/papers.cfm? abstract_id=3927791.
29. https://project7155832.tilda.ws/.
30. https://csec.uz/uz/news/mahalliy-yangiliklar/yurtimizda-mahalliy-siem-tizimining-dasturiy-taminoti-sertifikatlandi/.
31. https://ccdcoe.org/.
32. https://cyberleninka.ru/article/n/kiberprestupnost-kak-tenevoy-biznes.;
33. https://www.un.org/ru/desa/cybersecurity-demands-global-approach.