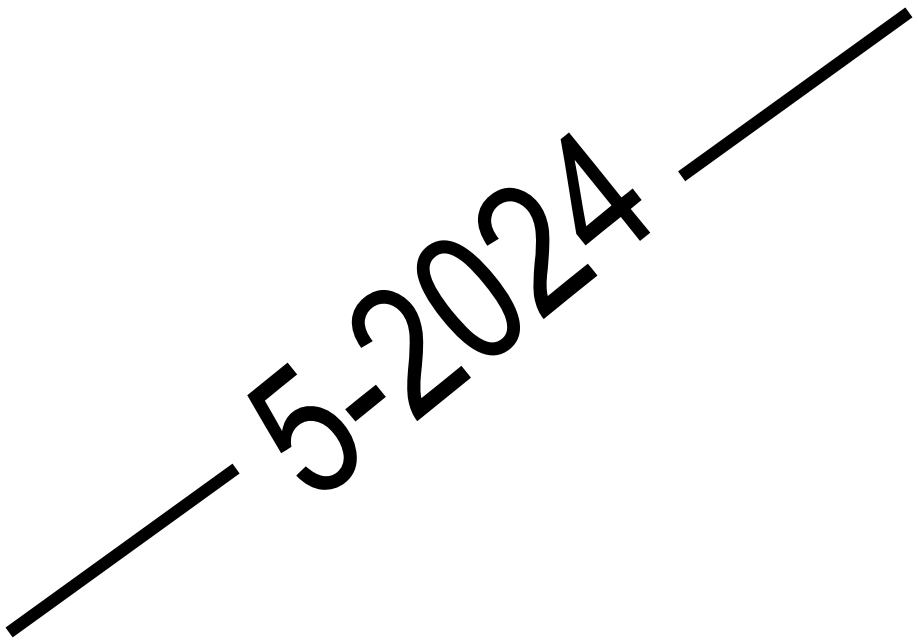
O‘ZBEKISTON RESPUBLIKASI

OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

FARG‘ONA DAVLAT UNIVERSITETI

FarDU. ILMIY XABARLAR-

1995-yildan nashr etiladi
Yilda 6 marta chiqadi



НАУЧНЫЙ ВЕСТНИК. ФерГУ

Издаётся с 1995 года
Выходит 6 раз в год

FarDU. Ilmiy xabarlar – Scientific journal of the Fergana State University

Volume 30 Issue 5, 2024-yil DOI: 10.56292/SJFSU/vol30_iss5/a23

UO‘K: 004.056:351.86

“XAVFSIZLIK” VA “KIBERXAVFSIZLIK” ATAMASINING MAZMUN-MOHIYATI VA JAMIYAT HAYOTIDA XAVFLILIK DARAJASINI BAHOLANISHI

СУЩНОСТЬ ТЕРМИНОВ «БЕЗОПАСНОСТЬ» И «КИБЕРБЕЗОПАСНОСТЬ» И ОЦЕНКА УРОВНЯ ОПАСНОСТИ В ЖИЗНИ ОБЩЕСТВА

THE ESSENCE OF THE TERMS "SECURITY" AND "CYBER SECURITY" AND ASSESSMENT OF THE LEVEL OF DANGER IN THE LIFE OF SOCIETY

Samijonov Azizbek Ismoiljon o‘g‘li
Farg‘ona davlat universiteti tadqiqotchisi

Annotatsiya

Ushbu maqolada kiberxavfsizlik tushunchasining mazmun-mohiyati va konseptual asoslari hamda “xavfsizlik” va “kiberxavfsizlik” atamasining mazmun-mohiyati tahlil qilingan. Shuningdek, kiberxavfsizlik butun insoniyat uchun global ahamiyatga ega bo‘lgan, uning obyektiv, amaliy ta’rifini shakllantirishning hayotiy zaruriyat ekanligi bilan tavsiflanuvchi zamonaviy jamiyatning noyob hodisasi ekanligi tahlil qilingan.

Аннотация

В данной статье анализируются сущность и концептуальные основы понятия кибербезопасности, а также значение терминов «безопасность» и «кибербезопасность». Также было проанализировано, что кибербезопасность – это уникальное явление современного общества, имеющее глобальное значение для всего человечества и характеризующееся тем, что формирование ее объективного, практического определения является жизненной необходимостью.

Abstract

This article analyzes the essence and conceptual foundations of the concept of cyber security, as well as the meaning of the terms "security" and "cyber security". It was also analyzed that cyber security is a unique phenomenon of modern society, which is of global importance for all humanity, and is characterized by the fact that it is a vital necessity to form an objective, practical definition of it.

Kalit so‘zlar: *kiberxafsizlik, xavfsizlik, axborot xavfsizligi, tahdid, kiber urush.*

Ключевые слова: *кибербезопасность, безопасность, информационная безопасность, угроза, кибервойна.*

Key words: *cyber security, security, information security, threat, cyber war.*

KIRISH

“Xavfsizlik” tushunchasining mohiyatini aniqlashtirish asosida “kiberxavfsizlik” atamasining mazmun-mohiyatini izohlashga harakat qilamiz. Bizningcha, kiberxavfsizlik butun insoniyat uchun global ahamiyatga ega bo‘lgan, uning obyektiv, amaliy ta’rifini shakllantirishning hayotiy zaruriyat ekanligi bilan tavsiflanuvchi zamonaviy jamiyatning noyob hodisasidir.

Kiberxavfsizlik - bu kompyuterlar, serverlar, veb-saytlar, mobil qurilmalar, elektron tizimlar, tarmoqlar va ma’lumotlarni zararli hujumlardan himoya qilish amaliyotidir. Kiberxavfsizlik - bu tizimlar, tarmoqlar va dasturiy ta’minotni raqamli hujumlardan himoya qilish bo‘yicha chora-tadbirlarni amalga oshirishdir. 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. Kiberxavfsizlik bo‘yicha samarali chora-tadbirlarni amalga oshirish allaqachon juda qiyin jarayon. Chunki bugungi kunda hujumlar amalga oshirilayotgan qurilmalar soni odamlar sonidan bir necha barobar ko‘p va kiberjinoyatchilar har kuni yangi ixtirolardan foydalanmoqda.

Kiberxavfsizlik odatda kompyuter xavfsizligi, tranzaksiya xavfsizligi, ma’lumotlar himoyasi, shaxsiy ma’lumotlar xavfsizligi, internet tarmog‘i xavfsizligi va hattoki har qanday signal uzatuvchi qurilmalar xavfsizligini o‘z ichiga oladi. Ushbu mavzularning keng tarqalishi va muhim ahamiyat kasb etishi sababi kiberhujumlar va tahdidlardir. Kiberhujumlar soni va turi oshgani sayin kiberxavfsizlik

tarmoqlari ham oshib bormoqda. 1980-yillardan boshlab “Kiber jinoyatchilar”, “Kiber dunyoda etika”, “Axloqiy kiber qaroqchilik” kabi tushunchalar paydo bo‘ldi. Kiberhujum turlari orasida pul yuvish va kiberjinoyatchilarning o‘z mahoratini namoyish qilish uchun qilingan hujumlari alohida o‘rin tutadi. Kiberxavfsizlik kiberhujumlarning sezilarli darajada oshishi tufayli davlatlar va kompaniyalar uchun juda muhim bo‘lib qoldi.

Kiberjinoyatlarning ko‘payishi davlat boshqaruvi, bank, transport, milliy xavfsizlik va boshqa tizimlarni takomillashtirish va butun dunyo bo‘ylab kibermudofaa choralarini kengaytirishni dolzarb qiladi.

Bugungi kunda butun dunyo bo‘ylab keng tarqalgan xakerlik tarmoqlari moliyaviy operatsiyalarni amalga oshiradi, fuqarolarning shaxsiy ma’lumotlariga kirishga erishadi, davlat organlarining rasmiy raqamlarini bosim ostida ushlab turadi. So‘nggi paytlarda ba’zi shtatlar saylov tizimiga kirish imkoniga ega bo‘lgani haqida ma’lumotlar tarqalmoqda. bu sohada tashviqot yaratishga urinishlar mavjud va shu bilan manipulyatsiya imkoniyatlari kengayadi. Xakerlar har qanday tizim strukturasida tizim xatolarini yoki tizim teshiklarini topadilar, ular bu ochilish sabablarini bilishadi. Afsuski, bir qator kompyuter foydalanuvchilari bilimsizlik va ehtiyotsizlik oqibatida moddiy va ma’naviy zarar ko‘rmoqda. Ushbu zararlardan qochish uchun siz ba’zi asosiy mavzularni bilishingiz va ba’zi xavfsizlik choralarini ko‘rishingiz kerak.

D.N.Karpovaning fikricha kiberjinoyatchilik – “Internet tarmog‘iga ega bo‘lgan har qanday texnik vositalar yordamida shaxs, tashkilot yoki davlatga iqtisodiy, siyosiy, axloqiy, mafkuraviy, madaniy va boshqa turdagi zarar yetkazish maqsadidagi ijtimoiy xavfli qilmishdir”[9]. E’tiborli jihati, Karpova shaxsga yetkaziladigan mafkuraviy zararni ham kiberjinoyatchilik deb hisoblaydi.

MATERIALLAR VA METODLAR

Bundan tashqari yana bir ishonchli manba, Birlashgan Millatlar Tashkilotining Giyohvand moddalar va jinoyatchilikka qarshi kurashish boshqarmasi tomonidan kiberjinoyatchilikka oid ishlab chiqilgan o‘quv-modulida “kiberjinoyatchilikka axborot-kommunikatsiya texnologiyalaridan (AKT) foydalangan holda yoki tarmoqlarga, tizimlarga, ma ’lumotlarga, veb-saytlarga, texnologiyalarga yo‘naltirilgan yoki jinoyat sodir yetishga yordam beradigan qonunni buzadigan harakat”[10], deb ta’rif berilgan.

Ushbu tushunchalardan farqli ravishda kiberjinoyat tushunchasiga quyidagicha ta’rif berish mumkin: kiberjinoyat – bu kompyuter tizimi, tarmog‘i, shuningdek kompyuter tizimi, tarmog‘iga ulanadigan boshqa vositalar orqali yoki ularning yordamida shaxs, jamiyat va davlatning moddiy va nomoddiy ne’matlariga qaratilgan axborot hujumi ko‘rinishidagi kibermuhitda sodir etilgan ijtimoiy xavfli qilmish.

M.Quronovning o‘zining “Biz anglayotgan haqiqat” kitobida “Diqqat, Internet” sarlavhasi ostida quyidagi fikrlarni bayon etgan: “Hali Internetning inson hayotidagi o‘rni haqida yakdil xulosa qilishga ertaroqqa o‘xshaydi. “Texnologiya biznesa. Connect” jurnali o‘zining 2003 yil 10-sonidagi “Informatsiya + natsiya” maqolasida xavotirli gaplarni yozdi. “Internetdan mustaqil foydalanuvchilarda, – deb yozadi jurnal, – o‘zini o‘zi barqaror identifikatsiya qilish, o‘ziga xoslik yo‘qola boradi. Odamning o‘zini anglashi xiralashadi yoki beqaror bo‘lib qoladi...”[11].

U.G‘afurovning ta’kidlashicha, “axborot iste’moli madaniyati, eng umumiy ma’noda, axborot oqimidan inson manfaatlari, kamoloti hamda jamiyat taraqqiyotiga xizmat qiluvchi ma’lumotlarni qabul qilish, saralash, tushunish va talqin etishga xizmat qiladigan bilim, qobiliyat va malakalar tizimini anglatadi” [12].

MUHOKAMA VA NATIJALAR

Kiberxavfsizlik bo‘yicha samarali chora-tadbirlarni amalga oshirish bugungi kunda juda qiyin, chunki bugungi kunda odamlar ko‘proq qurilmalarga ega bo‘lishiga qaramay, kiberjinoyatchilar tobora ko‘proq “ixtirochi” rolini o‘ynamoqda[1]. Shuningdek, bir qator kompyuter foydalanuvchilari bilimsizlik va ehtiyotsizlik oqibatida moddiy va ma’naviy zarar ko‘rmoqda. Ushbu zararlardan qochish uchun siz ba’zi asosiy mavzularni bilishingiz va ba’zi xavfsizlik choralarini ko‘rishingiz kerak.

Xodimlar, biznes jarayonlari va texnologiyalari kiberhujumlardan samarali himoyalanish uchun bir-birini to‘ldirishi kerak. Ushbu soha xodimlari axborot xavfsizligining asosiy tamoyillarini tushunishlari, kuchli parollarni tanlashlari, yuborilgan va qabul qilingan elektron pochta va unga biriktirilgan fayllarga e’tibor berishlari va ma’lumotlarning boshqa manbalarga xavfsiz zaxiralanishini ta’minlashlari kerak. 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.

Real hayotda bo‘lgani kabi virtual dunyoda ham xavfsizlik muhim ahamiyatga ega. Dunyoda har daqiqada kiberkosmosda 500 million hujum uyushtiriladi. Kiberxavfsizlik strategiyasini tayyorlagan O‘zbekiston ham albatta, bu xavf va xatarlardan xabardor va bu strategiyadan kelib chiqadigan qoidalarning amalga oshirilishi ularning oldini olishda muhim rol o‘ynaydi. O‘tgan davrda O‘zbekiston ham kiberxavfsizlik indeksini yaxshilagan. Global Cybersecurity Index davlatlarning kiberxavfsizlik bo‘yicha reytingini e’lon qildi. O‘zbekiston unda 182 davlat orasida 70-o‘rinni egalladi. Indeks beshta asosiy yo‘nalishda 82 ta savolni jamlagan. Ularning har biriga 20 ball beriladi. Bunda huquqiy, texnik va tashkiliy hamda imkoniyatlar va hamkorlikni rivojlantirish bo‘yicha choralarni o‘z ichiga oladi.

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”[2]. Bugungi kunda milliy iqtisodiyot va odamlarning turmush tarzi bilan bog‘liq bo‘lgan turli xil aloqa, energetika, transport va boshqa sanoat tarmoqlari o‘z faoliyatini ta’minlash uchun kompyuter tizimlariga tayanadi va fuqarolik kompyuter tizimlari Internetga juda bog‘liq bo‘lganligi sababli, keng ko‘lamli rejalashtirilgan tarmoq hujumlari keng qamrovli bo‘lishi mumkin. Chunki bu xujumlar mamlakatning normal iqtisodiy faoliyatini falaj qiladi.

Bu XX asrdagi an’anaviy elektron ushlash va XXI asrdagi kiber urush o‘rtasidagi farqni ko‘rsatadi, chunki u Internet passiv elektron ushlash bo‘limlariga kiberhujumlarni amalga oshirish imkoniyatini beradi.

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 alohida, shuningdek, 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 yaratishgan. Garchi bu davlatlar o‘zlarining asosiy maqsadi o‘z tarmoqlarini himoya qilish ekanligini ta’kidlagan bo‘lsalar-da, bu erda hujum operatsiyalari ham ko‘zda tutilgan.

XX asrning 60-yillarida axborot texnologiyalarining rivojlanishi natijasida operatsion tizimlarni to‘liq bilgan, uning chuqurligiga kirgan, kompyuterga har tomonlama qiziqqan, dasturlashni professional darajada biladigan kompyuter mutaxassislari – xakerlar paydo bo‘ldi. Qo‘shma Shtatlar 2011 yilda erkin savdo va ijtimoiy-iqtisodiy rivojlanish uchun ishonchli, xavfsiz va ochiq muhitni yaratish imkonini beruvchi kiberxavfsizlikning xalqaro asoslarini shakllantirish bo‘yicha hujjat tayyorladi. Ushbu hujjat bir nechta asosiy tamoyillarni tavsiflaydi. Birinchi o‘rin - iqtisodiy munosabatlar hisoblanadi. Shu boisdan ham Qo‘shma Shtatlar shaxsiy ma’lumotlarni, jumladan, tijorat sirlarini himoya qilish orqali Internet orqali erkin savdoni yaratishni taklif qilmoqda. Yana bir muhim ustuvor vazifa – kibermakonda xalqaro axloq kodeksini yaratish masalasidir. Loyiha mualliflarining fikricha, “bunday kodning mavjudligi xorijlik xakerlik hujumlaridan himoyalanish imkonini beradi. Yana bir yo‘nalish esa kiberjinoyatchilikka qarshi kurashga bag‘ishlangan”[3].

AQSH e’tiborni muayyan jinoyatlarga qaratishga va internetga kirishni cheklamaslikka chaqiradi. Shuningdek, xavfsiz muhitni yaratish imkoniyati bo‘lmagan mamlakatlarga yordam ko‘rsatish ko‘zda tutilgan. “Strategiya AQSHning barcha yirik vazirliklarini qamrab oladi, ularning barchasiga xorijiy davlatlardagi o‘xshash vazirliklar ishtirokida o‘zaro hamkorlik tamoyillarini yaratish vazifasi yuklatilgan”[4].

Kiber urushikki toifaga bo‘linadi: kiber josuslik va kiberhujumlar. Kiber-josuslik faoliyati odatda kuch bilan qasos olishga olib kelmaydi; ammo, kiber-josuslik faoliyati va kiberhujum faoliyati o‘rtasida aniq chegara yo‘q va doimiy kiber-josuslik faoliyati ba’zan kiberhujumlarga tayyorgarlik bosqichidir. Agar biror davlatning harbiy razvedka boshqarmasi boshqa davlat internetini yo‘q qilishga yoki milliy iqtisodiyot va xalq turmushi bilan chambarchas bog‘liq bo‘lgan boshqa davlatlarning hukumati, harbiy yoki xususiy korxonalarining veb-saytlari va ma’lumotlar bazalarini yo‘q qilishga urinsa, odatda bunday kiberhujumlar sodir bo‘ladi. Amerika Qo‘shma Shtatlari, Buyuk Britaniya, Kanada va boshqa davlatlar kibermudofaa nuqtai nazarini o‘zgartirdi.Oddiy kibermudofaa

o‘tkazishdan tashqari, ular nishonning tabiati, vaziyatning ta’siri va samaradorligi kabi mezonlarga alohida e’tibor qaratadilar. Ular xakerlar va kiberjinoyatchi tashkilotlarga qarshi faol kiberhujumlar uyushtiradilar.

AQSH harbiylari kibermakon va kiberoperatsiyalarda “burilish nuqtasida” turibdi, bu asosan quyidagi to‘rt jihatda aks etadi: Birinchidan, kiberxurujlarning oldini olish nuqtai nazaridan, kiberxavfsizlik tizimini hisobga olishdan tashqari, u ham xodimlarning omillarini, ya’ni kiberhujumlarning oldini olishni ko‘rib chiqadi. Raqiblarga ta’sir qilish kiberkosmosdagi operatsiyalar qanday amalga oshirilayotganini tarozida ko‘radi; ikkinchidan, DoDning kiber haqidagi tushunchasi rivojlanmoqda, Amerika Qo‘shma Shtatlariga qarshi zararli faoliyatni oldini olish uchun axborot operatsiyalari va kiberoperatsiyalarni yana-da yaqinroq bog‘laydi; keng qamrovli to‘xtatuvchi ta’sirga erishish uchun boshqa sohalarning roli; To‘rtinchidan, kibermakondagi vaziyat tez o‘zgarmoqda, shuning uchun AQSH harbiylari ushbu sohada “doimiy ishtirok etish” pozitsiyasini saqlab turishi kerak.

Jahon hamjamiyati yangi davr — axborot jamiyati davriga kirib, kompyuterlar va telekommunikatsiya tizimlari inson va davlat hayotining barcha sohalarini qamrab olgan. Ammo insoniyat o‘zini telekommunikatsiya va global kompyuter tarmoqlari xizmatiga qo‘yib, bu texnolog iyalarni suiiste’mol qilish uchun qanday imkoniyatlar yaratilishini oldindan sezmagan. Bugungi kunda virtual makonda faoliyat yuritayotgan jinoyatchilar qurbonlari nafaqat odamlarga, balki butun davlatlarga aylanishi mumkin. Shu bilan birga, axborot xavfsizligiga qarshi jinoyatlarni bir necha jinoyatchilar uyushmasi yoki guruhi sodir qilishi mumkin. Kibermuhitda sodir yetilgan jinoyatlar soni kompyuter tarmoqlaridan foydalanuvchilar soniga mutanosib ravishda o‘sib bormoqda va Xalqaro jinoyat politsiyasi tashkiloti – “Interpol hisob-kitoblariga ko‘ra, global internet tarmog‘ida ushbu jinoyatchilikning o‘sish sur’ati sayyoramizda eng tezkor hisoblanadi”[5].

Bugungi kunda kiberjinoyatchilikda muayyan shaxsning yoki obyektning geografik joylashgan nuqtasi to‘g‘risida xabar tarqatish, sh axsiy ma’lumotlar bazasini buzib kirish kabi xizmatlar ommalashgan. Xakkerlar bu kabi ma’lumotlarni internet va ijtimoiy tarmoq foydalanuvchilari tomonidan turli elektron resurslarga ularning foydalanish shartlarini o‘qimasdan turib kirishlari evaziga olishmoqda.

Axborot-texnologiyalar vositasida sodir qilingan jinoyatlar, allaqachon rivojlangan xorijiy mamlakatlarda “kiberjinoyatlar” deb nomlanadi va ushbu ijtimoiy xavfli qilmishlarga qarshi kurashish, oldini olish, uning keyingi faoliyatiga to‘sqinlik qilish kabi chora-tadbirlar qonunchiligida belgilangan. Umuman olganda, kiberjinoyatlarning o‘ziga xos xususiyati quyidagilar: ushbu toifadagi jinoyatlar makon tanlamay, uni istalgan payt dunyoning turli tomonlaridan kutish mumkin; muntazam ravishda har kuni yangi va oldingilaridan ancha xavfliroq bo‘lgan virus va boshqa zararli dasturlarning yaratilishi; kiberjinoyatlarga qarshi kurashadigan organlarda malakali va ushbu sohada mukammal bilimlarga ega mutaxassislar mavjud emasligi va buning natijasida jinoyatning kech aniqlanishi; kiberjinoyat natijasida muayyan mulk emas, balki axborotlarga nisbatan mulkchilik huquqi yo‘qotiladi; axborotlarni qayta ishlash jarayonida yo‘l qo‘yilgan xatolik o‘z vaqtida kuzatilmaydi va tuzatilmaydi, natijada kelgusida sodir bo‘ladigan xatolarning oldini olib bo‘lmaydi[6]; sodir etiladigan kompyuter jinoyatlari o‘z vaqtida e’lon qilinmaydi (hisoblash tarmoqlarida kamchiliklar mavjudligini boshqalardan yashirish, muassasa ishchanlik obro‘yini saqlab qolish va boshqa maqsadlarda); kiberjinoyatni tergov qilish hamda ochishning o‘ziga xos qiyinligi, juda katta zararga olib kelishi, jinoyatchilarga qarshi kurashish va uning profilaktikasi uchun yagona huquqiy asosning mavjud emasligi kabilar.

So‘nggi yillarda ommaviy axborot vositalarida “kiberjinoyat” tushunchasiga borgan sayin ko‘proq duch kelayotgan bo‘lsak-da, ushbu tushunchaga sinonim sifatida mamlakatimizda “kompyuter jinoyatlari” yoki “axborot texnologiyalari sohasidagi jinoyatlar” tushunchalari qo‘llaniladi. Ammo aksariyat mualliflar ““kiberjinoyat” tushunchasini “kompyuter jinoyatlari” tushunchasidan farq qilishini, ushbu tushuncha axborotlashtirish sohasidagi barcha jinoyatlarni qamrab olishini, shu orqali “kompyuter jinoyatlari”ga nisbatan kengroq tushuncha ekanligini”[7] ta’kidlashgan. Bundan ko‘rinadiki, kiberjinoyat kompyuterdan foydalanish yoki kompyuter, global tarmoq orqali sodir qilinadigan jinoyatdir[8].

XULOSA

Xullas, birinchidan, bugungi kunda dunyodagi ilg‘or kiberhimoya 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 va 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. Ikkinchidan, hozirda 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 tadbirlar o‘tkazilmoqda.

ADABIYOTLAR RO‘YXATI

1. Курилкин А.В. Информационные и кибернетические операции как инструмент реализации внешней политики : формы, методы, технологии : диссертация ... кандидата политических наук. - Москва, 2021. - 207 с. (Kurilkin A.V. Information and cybernetic operations as a tool for implementing foreign policy: forms, methods, technologies: dissertation ... candidate of political sciences. - Moscow, 2021. - 207 p.)

2.https://rus.lb.ua/economics/2012/01/27/133936_oon_provedet_globalnoe.html

3. Батуева Е.В. Американская концепция угроз информационной безопасности и ее международно-политическая составляющая : диссертация ... кандидата политических наук. - Москва, 2014. - 207 с.(Batueva E.V. American concept of threats to information security and its international political component: dissertation ... candidate of political sciences. - Moscow, 2014. - 207 p.)

4. Виловатых А.В. Информационное противоборство в политическом процессе : тренды цифровой реальности : диссертация ... доктора политических наук. - Москва, 2021. - 347 с.(Vilovatykh A.V. Information confrontation in the political process: trends of digital reality: dissertation ... doctor of political sciences. - Moscow, 2021. - 347 p.)

5. https://www.interpol.int/Crimes/Cybercrime

6. Ro‘ziyev R.N., Salayev N.S. Kiberjinoyatchilikka qarshi kurashishga oid milliy va xalqaro standartlar. Monografiya. – Toshkent: TDYUU, 2018, 6-bet.(Roziyev R.N., Salayev N.S. National and international standards for combating cybercrime. Monograph. - Tashkent: TDYUU, 2018, p. 6.)

7. Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза.// Криминология: вчера, сегодня, завтра. – 2012 г. – (24). – С.47.; (Nomokonov V.A., Tropina T.L. Cybercrime as a new criminal threat.// Criminology: yesterday, today, tomorrow. – 2012. – (24). – P.47.;)

8. Киберпреступность: криминологической, уголовно правовой, уголовно-процессуалный и криминалистический анализ. / Науч. ред. И.Г.Смирного. – М., 2016. – С. 34.(Cybercrime: criminological, criminal law, criminal procedure and forensic analysis. / Scientific ed. I.G.Smirny. - M., 2016. - P. 34.)

9. Gurcke M. Understanding Cybercrime: A Guide for Developing Countries. ITU, 2009.

10. Карпова Д.Н. Киберпреступность: глобальная проблема и ее решение. Власть, 2014, ст.47.(Karpova D.N. Cybercrime: a global problem and its solution. Vlast, 2014, p.47.)

11. Киберпреступность. Модуль 1. Введение в киберпреступность.// Образование во имя правосудия серия университетских модулей.// (Cybercrime. Module 1. Introduction to Cybercrime.// Education for Justice University Module Series.//)

12. Управление Организации Объединенных Наций по наркотикам и преступности., Вена, 2019. (United Nations Office on Drugs and Crime, Vienna, 2019.)

13. Quronov M. Biz anglayotgan haqiqat. – T.: Ma’naviyat, 2008. –B. 5-6.(Kuronov M. The truth we perceive. - T.: Ma'naviyat, 2008. -B. 5-6.)

14. G‘afurov U. Globallashuv sharoitida yoshlarni din niqobidagi mafkuraviy tahdidlardan asrashda Internetdan samarali foydalanishning dolzarb masalalari. // “Armiya – davlat tayanchi, tinchlik kafolati”. Qurolli Kuchlar tizimidagi tarbiyaviy ishlar organlari hamda targ‘ibotchilar uchun uslubiy qo‘llanma. – T.: “Sano-standart” nashriyoti, 2013. – B. 285.(Gafurov U. Current issues of effective use of the Internet in protecting young people from ideological threats in the guise of religion in the context of globalization. // "The army is the support of the state, the guarantee of peace." Methodological guide for educational institutions and propagandists in the Armed Forces. - T.: "Sano-standard" publishing house, 2013. - P. 285.)