ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889,
2024-6.875 ResearchBib IF: 9.948 / 2024

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-5, ISSUE-5

Diplomat university xalqaro munosabatlar va iqtisodiyot fakulteti xalqaro munosabatlar va zamonaviy siyosiy jarayonlar yo`nalishi 1-kurs magistratura talabasi Atxamjonov Abbosxon Atxamjon o`gli.

“YANGI O‘ZBEKISTON TASHQI SIYOSATIDA KIBERJINOYATLARGA QARSHI KURASH SIYOSATI, XUSUSIYATLARI”

ANNOTATSIYA

Mazkur maqola Yangi O'zbekistonning tashqi siyosatida kiberjinoyatlarga qarshi kurashish siyosatining xususiyatlarini tahlil qiladi. Kiberjinoyatlar dunyo miqyosida xavf-xatarlarni kuchaytirib, davlatlar xavfsizligini tahdid qiluvchi omilga aylangan. Shuningdek, axborot-kommunikatsion texnologiyalar va raqamli xavfsizlik masalalari haqida ham so'z yuritiladi. Maqolada kiberjinoyatlarga qarshi kurashishda mamlakatlar o'rtasidagi hamkorlikning zarurati va huquqiy tizimni yaxshilash bo'yicha takliflar keltirilgan.

Kalit so‘zlar: Yangi O'zbekiston, tashqi siyosat, kiberjinoyatlar, xavfsizlik, xalqaro hamkorlik, axborot-kommunikatsiya.

АННОТАЦИЯ

В данной статье рассматриваются виды киберпреступлений, их социальные и экономические последствия, а также важность международного сотрудничества для эффективной борьбы с ними. Также обсуждаются информационно-коммуникационные технологии и вопросы цифровой безопасности. В статье подчеркивается необходимость сотрудничества между странами в борьбе с киберпреступностью и предложения по совершенствованию правовой системы.

Ключевые слова: Новый Узбекистан, внешняя политика, киберпреступления, безопасность, международное сотрудничество, информационно-коммуникационные технологии, цифровая безопасность, правовые проблемы, кибербезопасность.

ABSTRACT

This article analyzes the features of the policy of combating cybercrime in the foreign policy of New Uzbekistan. Cybercrime has become a global threat and a factor threatening the security of states. It also discusses the issues of information and communication technologies and digital security. The article presents the need for cooperation between countries in combating cybercrime and proposals for improving the legal system.

Keywords: New Uzbekistan, foreign policy, cybercrime, security, international cooperation, information and communication technologies, digital security, legal issues, cybersecurity.

Kirish.

Zamonaviy global muhitda kiberjinoyatlar har bir davlatning xavfsizligi uchun muhim tahdidga aylanib bormoqda. Raqamli texnologiyalar va axborot-kommunikatsiya vositalarining tez sur'atlar bilan rivojlanishi, kiberjinoyatchilik faoliyatini kengaytirib, davlatlarning ichki va tashqi xavfsizligiga salbiy ta'sir ko'rsatmoqda. Ayniqsa, so‘nggi yillarda «Yangi O‘zbekiston» siyosatida turli ustuvor yo‘nalishlarda ijobiy o‘zgarishlar yuz berdi desak, adashmaymiz. Ammo shu bilan

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889,
2024-6.875 ResearchBib IF: 9.948 / 2024

birgalikda ommaviy xavf- xatarlar soni ortib bormoqda. Ayni kunlarda global xavflar sirasiga kiruvchi kiberjinoyatlarga qarshi kurashish masalalariga ham jiddiy e'tibor berish ahamiyatga molikdir. Bugungi kunda bu jinoyatlar dunyo bo'ylab davlatlar xavsizligiga tahdid qilayotgan muammo, bir so'z bilan aytganda esa yangi avlodni tashvishga qo'yuvchi muammolardan biriga aylangan. Ushbu harakatlarning har bir davlatga va millatga ijtimoiy, iqtisodiy ta'sirlari o'ta jiddiy bo'lib, unga qarshi qonuniy va samarali kurashish, har tomonlama integratsiyalashgan yondashuvlarni amalga ochirish lozim. O'zi kiberjinoyat nima? Dastlab, kiberjinoyatlar xususida to'xtalish joiz.

Kiberjinoyatlar — bu internet va raqamli tarmoqlar orqali sodir etiladigan jinoyatlar. Ushbu jinoyatlar turkumiga quyidagi asosiy turlar kiradi:

- Hujumlar: DDoS (Distributed Denial of Service), phishing, malware (zararli dasturlar) kabi hujumlar.
- Tashkilotlar va korporatsiyalar uchun tahdid: Banking, moliya sektori, sog'liqni saqlash, ta'lim va boshqa tizimlarga yo'naltirilgan xakerlik hujumlari.
- Shaxsiy yoshdagi kiber jinoyatlar: Odamlarning shaxsiy ma'lumotlarini o'g'irlash yoki uzoq masofadan shantaj qilish. Uning xususiyatlari va tahdidli ko'rinishlari haqida gapiradigan bo'lsak, kiberjinoyat -axborot texnologiyalari va internet resurslaridan noqonuniy ravishda, shaxsiy manfaatlarni ko'zlab, zararli maqsadda foydalanish, sodda qilib aytganda, bu turdagi jinoyatni kompyuter qarshisida o'tirib, minglab kilometr uzoqlikdagi mintaqada joylashgan biror bir tashkilotning mablag'ini o'marish orqali sodir etish mumkin.

Kiberjinoyatlar — axborot tizimlari, tarmoqlar va axborot infrastrukturasiga ta'sir qiluvchi tajovuzlar va jinsiy jinoyatlar. O'zbekiston o'z iqtisodiyoti, ijtimoiy hayoti va milliy xavfsizligiga tahdid soladigan kiberjinoyatlarni yengish uchun qulayliklar yaratishga muhtoj. Kiberjinoyatlarning asosiy turlari quyidagilar:

— Ma'lumotlarni o'g'irlash: Bank hisob raqamlarini, shaxsiy ma'lumotlarni va boshqa maxfiy axborotni o'g'irlash.

— Kiber hujumlar: Tashqi manbalardan foydalangan holda tashkilotlar va muassasalar serverlariga hujumlar.

— Firibgarlik: Internet orqali firibgarlik, masalan, soxta veb-saytlar orqali.

Jahonda sodir etiluvchi jinoyatlarning ichida kiberjinoyat to'ĸtinchi o'rinni egallagan. Shuningdek viruslar yordamida zarar yetqazuvchi dasturlarni tarqatish, parollarni buzib kirish, kredit karta va boshqa bank rekvizitlaridagi raqamlarni o'g'irlash, internet orqali qonunga zid axborotlarni tarqatish kiberjinoyatning asosiy turlariga kiradi. Jumladan, o'zganing ID parolini o'g'irlash va jinoiy maqsadda boshqa shaxsga tegishli shaxsiy ma'lumotlarni aldab olish harakatlari elektron hukumat va elektron tijorat xizmatlarining rivojlanishiga qarshi asosiy tahdidlardan biri hisoblanadi.

Kiberjinoyatlar bilan bog'liq statistikalar har yili o'zgarib turadi va ko'pincha davlatlar va tashkilotlar tomonidan vakolatli idoralar, xizmatlar va kompaniyalar tomonidan to'planadi. O'zbekiston va dunyo bo'yicha kiberjinoyatlarga doir statistikalar quyidagilar bilan ifodalanishi mumkin:

O'zbekistonda kiberjinoyatlar statistikasi to'g'risida aniq ma'lumot olish qiyin bo'lishi mumkin, chunki bu ko'rsatkichlar ko'pincha rasmiy hisobotlarda yoki ijtimoiy-iqtisodiy tadqiqotlar orqali berilmaydi. Biroq, davlat idoralari (masalan, Iqtisodiyot va sanoat vazirligi, Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi) va kiber xavfsizlik bo'yicha tashkilotlarning ma'lumotlariga asoslanib, quyidagi ko'rsatkichlar kuzatilishi mumkin:

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889,
2024-6.875 ResearchBib IF: 9.948 / 2024

— 2022-2023 yillar davomida: Kiberjinoyatlar soni har yili ortib borayotganligi haqida ma'lumotlar mavjud. Statistikalar bo'yicha, O'zbekistonda 2023 yilga kelib, kiberjinoyatlar sonining 30-50% gacha oshganligi haqida taxminlar mavjud.

Dunyo bo'yicha kiber jinoyat statistikasi esa quyidagi ma'lumotlarni o'z ichiga olishi mumkin: Kiber jinoyatlar statistikasi: 2021 yilda global kiberjinoyatlar soni 2020 yilga nisbatan 50% dan ko'proq oshganligi haqida turli xabarlar mavjud.

- Phishing hujumlari: McAfee kompaniyasi ma'lumotlariga ko'ra, 2021 yilda phishing hujumlari 61% oshgan.
- Ransomware (ma'lumotlarni shantaj qilish) hujumlari: Cybereason tadqiqotlariga ko'ra, ransomware hujumlari 2020 yilga nisbatan 150% ortgan.

Kiberjinoyatlar reytingida Rossiyadan keyingi o‘rinda Ukraina, Xitoy, AQSh va Nigeriya bormoqda, deya xabar beradi Oksford universiteti so‘nggi 3 yil davomida o‘tkazilgan tadqiqotga tayanib.

Uch yil davomida o‘tkazilgan tadqiqotda kiberjinoyatlarning eng muhim manbalari baholandi va tarixda birinchi marta Jahon kiberjinoyat indeksi (WCI) bo‘yicha mamlakatlar reytingi tuzildi. Unda butun dunyo bo‘ylab kiberjinoyatlar bo‘yicha 92 ta yetakchi ekspertlarning baholaridan foydalanilgan. Ulardan kiberjinoyatlarning beshta asosiy turining eng muhim manbalarini aniqlash va kiberhujumlar natijalari hamda xakerlarining professionalligi va texnik imkoniyatlariga ko‘ra mamlakatlarni tartiblash so‘ralgan.

Yuqorida keltirilgan statistik ma’lumotlar kiberjinoyatlarning global muammoga aylanganini ko'rsatadi. O'zbekistonda kiberjinoyatlarga oid aniq statistikani ko'rish murakkab bo'lishi mumkin, lekin xalqaro statistikalar va tadqiqotlar, kiber jinoyatlarga qarshi kurash bo'yicha chora-tadbirlarni kuchaytirishni talab qiladi. O'zbekiston ham kiberxavfsizlikni ta'minlashda xalqaro tajribani o'rganishi va kiberjinoyatlarga qarshi kurashishda jamoatchilik va davlat organlari birgalikda faoliyat olib borishi muhimdir.

Axborot kommunikatsion texnologiyalari aholiga ancha qulaylik yaratdi. Atrofga nazar solib fikrlaydigan bo‘lsak, songgi yillar mobaynida texnik o‘zgarishlar rivoj topgani, bank kartalari, kredit kartalarning takomillashuvi, axborot kommunikatsion texnologiyalari (AKT) rivoji, ularni raqamlshtirish tendensiyalari o‘sib borganini ko‘rishimiz mumkin. Elektr ta’minoti, transport infratuzilmasi, harbiy xizmat deymizmi yoki logistika deyarli barcha sohalar axborot texnologiyalaridan foydalanishga bog‘langan. Bundan ko‘rinadiki, axborot kommunikatsion texnologiyalarning jamiyatga ta’siri asosan, axborot manbayi hisoblanadi.

Tahliliy jihatdan qaraydigan bolsak, axborot uzatishlarning o‘sishi yangi va jiddiy tahdidlar bilan birga keldi. Bu harakatlar esa jamiyatning barqaror faoliyati rivojiga katta to‘siqlardan biri. Bu to‘siqlar axborot infratuzilmasi va internet xizmatlariga nisbatan uyishtirilgan hujumlarda o‘z aksini topadi. Misol qilib aytadigan bo‘lsak, xakkerlik hujumlari, rivojlanayotgan davlat yoki kompaniyaning internet tarmog‘iga buzg‘unchilik orqali kirib olish va g‘alizona ta’siri bilan bilan ko‘rinadi. Yil hisobida ko‘rib chiqsak, 2024-yilda 7 oy davomida 577 mingta axborot texnologiyalari sohasidagi jinoyatlar qayd etilgan.

Kiberjinoyatlar zamonaviy dunyoda har bir davlatning xavfsizligiga tahdid soluvchi muammolarga aylangan. Ular nafaqat iqtisodiyotga salbiy ta’sir ko’rsatishi mumkin, balki davlatlar o'rtasidagi ishonch va barqarorlikka xavf tug'diradi.

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889,
2024-6.875 ResearchBib IF: 9.948 / 2024

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-5, ISSUE-5

1. Kiberjinoyatlarning global holati

Dunyoda kiber jinoyatlar soni tobora ortib bormoqda. Bunga sabab:

- Raqamli transformatsiya: Davlatlar raqamli iqtisodiyot va axborot infratuzilmasini rivojlantirgandan so'ng, kiber jinoyatchilar uchun yangi imkoniyatlar paydo bo'ladi.
- Texnologiyalarni rivojlantirish: Sun'iy intellekt, bulutli hisoblash va IoT kabi yangi texnologiyalar ham kiber jinoyatlarning o'sishiga sabab bo'lmoqda.

O'zbekistonning kiber xavfsizlik siyosati

O'zbekistonning kiber xavfsizlik siyosati asosan quyidagi xususiyatlarga ega:

— Xalqaro hamkorlik: O'zbekistonning kiberjinoyatlarga qarshi kurashishda xalqaro tashkilotlar va mamlakatlar bilan hamkorlik o'rnatishi zarur. Bu, masalan, BMT va SHHT kabi tashkilotlar orqali amalga oshiriladigan global dastur va tashabbuslarni o'z ichiga oladi.

— Huquqiy tizimni yaxshilash: O'zbekistondagi kiberjinoyatlarga qarshi kurashda ma'muriy va jazoviy qonunchilikni kuchaytirish zarur. Hukumat kiberjinoyatlarga qarshi kurashda yangi qonunlar qabul qilish va mavjud qonunlarni takomillashtirishni davom ettirmoqda.

— Axborot texnologiyalarini rivojlantirish: O'zbekiston ichki kiber xavfsizlikni ta'minlash va erkin raqamli muhit yaratish uchun zamonaviy axborot texnologiyalarini jalb qilishi kerak. Bunga kiber himoya texnologiyalarini joriy etish va tadqiqotlarni kuchaytirish kiradi.

3. Kiber xavfsizlikdagi kooperatsiyaning zarurati

Kiberjinoyatlarga qarshi kurashishda mamlakatlar o'rtasida kooperatsiya quyidagi jihatlarda zarur:

— Ma'lumot almashish: Kiber tahdidlar haqida ma'lumot almashish orqali davlatlar bir-birini himoya qilishi mumkin. Ogohlantirish va xavf-xatarlarni baholash orqali samarali kurashish imkoniyatlari yaratiladi.

— Birgalikda tayyorgarlik: Tashqi tahdidlarga qarshi harakat qilishda bir-biriga yordam berish va tayyorgarlik o'rnatish orqali davlatlar o'z xavfsizliklarini oshirishi mumkin. Bunda kiber xavfsizlik bo'yicha ta'lim va treninglarni birgalikda o'tkazish muhimdir.

4. Huquqiy tizimni yaxshilash bo'yicha takliflar

O'zbekistonda kiberjinoyatlarga qarshi kurashishda huquqiy tizimni yaxshilash uchun quyidagi takliflar keltirilishi mumkin:

— Kiberjinoyatlar bo'yicha alohida qonun: Kiber jinoyatlarga alohida yondashuv va huquqiy nazoratni ta'minlash uchun maxsus qonunlar va rezolyutsiyalar ishlab chiqilishi zarur.

— Kadrlar tayyorgarligi: Kiberjinoyatlarga qarshi kurashda qulay qonunchilik tayyorgarligini talab qiluvchi malakali kadrlar tayyorlash dasturlarini joriy etish.

— Ommaviy xabardorlik va ta'lim: Kiberxavfsizlik va himoya haqida aholining tushunchasini oshirish uchun xabardorlik kampaniyalarini o'tkazish va ta'lim dasturlarini ishlab chiqish muhim.

Vaziyatlar tahlilidan namoyon bo‘lganidek, axborot himoyasi bilan bardavom shug‘ullanishni hamisha bosh maqsadimizga aylantirmas ekanmiz, bu xatarlarni bartaraf eta olmaymiz. Kiberjinoyatlarga qarsi kurashishning samarali usullaridan biri “xalqaro hamkorlik” qilishdir. Faqat texnik sabablar jinoyatchilikni oldini olish uchun kamlik qiladi samarali natija uchun hamkorlikka ega har bir davlat huquqni muhofaza qilish organlari kiberjinoyatchilik tekshiruvini oshirish va jazolashni takomillashtirishi hamda internet tarmoqlarida sodir etilgan jinoyatlardan kelib chiqadigan

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889,
2024-6.875 ResearchBib IF: 9.948 / 2024

huqiqiy muammolarni xalqaro miqyosda hal etish zarur. Kiberjinoyatchilar ayrim nufuzli kompaniyalarga hujum uyushtirib xaridorlarning yo‘qolishi bilan qo‘rqitadi. Bundan sarosimaga tushgan kompaniya holatni ommaga bayon etmasligi bilan jinoyatchilikni takomillashuviga hissador bo‘lib qoladi. Shu bois xalqaro hamkorlik shartnomalarini belgilab kiberxavfsizlik xodimlarini sonini yana ko‘paytirish Va ular uchun maxsus alohida darsliklar tashkil etish ularning malakasini rivojlantirish uchun mamlakatlar o‘zaro fikr almashishlari kerak.

Xususan, xalqaro miqyosda texnik himoya tizimlarini ishlab chiqarish va har bitta davlat aholisini kiberjinoyatchilik qurboni bo‘lishdan saqlanish bo‘yicha seminar-treninglar o‘tqazish, aholini turli noaniq saytlarga kirishdan ogohlantirish, kiberxavsizlik strategiyasini ishlab chiqish va tadbiq etish jinoyatga qarshi kurashda muhim elementlardan hisoblanadi. Shuningdek, xalqaro hamkorlikda boshqa davlatlarning jinoyatga qarshi kurash strategiyasini kuzatishimiz va osh davlatdan o‘rnak olishimiz, asosiy e’tiborni himoyaga qaratishimiz lozim. Misol voyaga yetmaganlar uchun alohida internet tarmog‘i yaratilishi (Rossiya federatsiyasi misolida) va voyaga yetmaganlar uchun internetdan foydalanish soatini tartibga solish (Xitoy misolida)

Shu singari O‘zbekiston ham o‘z tarmog‘ini yaratishi va uni muhofaza etish uchun malakali mutahasislar bilan ta’minlashi rejasini ishlab chiqishi kerak. Shuningdek tarmoq turli bo‘limlardan iborat bo‘lishi masalan yoshiga qarab kantentlar joylashuvi amalga oshirilishi lozim. Bu esa tarmoq tezligini ham ta’minlab beradi. Xulosa o‘rnida aytadigan bo‘lsak O'zbekistonning kiberxavfsizlikka oid

tashqi siyosatining muvaffaqiyati,nafaqat

milliy xavfsizlikni ta'minlash, balki dunyo miqyosida barqarorlikni saqlash uchun muhim ahamiyatga ega bo'ladi.

Xulosa qilib aytadigan bo’lsak, “Yangi O'zbekiston” tashqi siyosatida kiberjinoyatlarga qarshi kurash, global xavfsizlikni ta'minlashda muhim rol o'ynaydi. Ushbu siyosat ko'p tomonlama yondashuvni, xalqaro hamkorlikni va zamonaviy texnologiyalarni o'z ichiga olishi zarur. Kiberjinoyatlarga qarshi kurashish yo'lidagi harakatlar, bir tomondan, mamlakat ichidagi xavfsizlikni ta'minlaydi, ikkinchi tomondan esa, O'zbekistonning mintaqaviy va global miqyosdagi obro'sini oshiradi. Kelajakda, kiber xavfsizlik sohasida yetakchilikni saqlab qolish maqsadida kompleks yondashuvlar va ilg'or innovatsion yechimlar kerak bo'ladi. Bu esa kelajakda O'zbekistonning kiberjinoyatlarga qarshi kurashda xalqaro tajribalardan o'rganish va zamonaviy texnologiyalarni joriy etishni, shuningdek, ijtimoiy xabardorlikni oshirishga qaratilgan dasturlar ishlab chiqishni taqozo etmoqda.

Foydalanilgan adabiyotlar ro’yxati:

1.Salayev N.S., Ro'ziyev R.N Kiberjinoyatchilikka qarshi kurashishga oid milliy va xalgaro standartlar. Monografiya ., - T.: TDYU, 2018, 139-b.

2.Карпова Д.Н. Киберпреступность: глобальная проблема и её решение. //Власть. Ne8. 2014.

3.Kiber huquq - huquq sohasi sifatida: risola / tuzuvchilar R.R.Shakurov,
M.M. Vohidov. - Toshkent: O‘zbekiston Respublikasi Adliya vazirligi qoshidagi
Yuristlar malakasini oshirish markazi

4. O‘zbekiston Respublikasining Qonuni Kiberxavfsizlik to‘g‘risida Qonunchilik palatasi tomonidan 2022-yil 25-fevralda qabul qilingan Senat tomonidan 2022-yil 17-martda ma’qullangan.

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889,
2024-6.875 ResearchBib IF: 9.948 / 2024

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-5, ISSUE-5

Foydalanilgan saytlar ro’yxati:

1. O‘zbekiston raqamli texnologiyalari vazirligi rasmiy sayti https://gov.uz/ru/digital
2. BMT Kiber Xavfsizlik Tashabbuslari
BMT rasmiy sayti: Basic facts about the global cybercrime treaty | United Nations
3. Jahon kiberjinoyat indeksi (WCI) World Cybercrime Index (WCI) - Rau's IAS
4. Interpol Xalqaro kiber jinoyatchilik hisobotlari: INTERPOL | The International Criminal Police Organization
5. World Economic Forum Kiber xavfsizlik va global tahdidlar bo'yicha ma'lumotlar: [weforum.org](https://www.weforum.org)
- Kiber xavfsizlik va tushuncha xavflari haqida global nuqtai nazar.