

ZAMONVIY XALQARO MUNOSABATLARDAKIBERXAVFSIZLIK MUAMMOSI

Mohigul Rahmanovna Mayusupova

“Xalqaro munosabatlar va jahon siyosati” mutaxassisligi 2-kurs magistranti
Toshkent davlat sharqshunoslik universiteti
e-mail: mohigulmayusupova@gmail.com

Annotatsiya: Raqamli davrda kiberxavfsizlik xalqaro munosabatlarda xalqlarning o‘zaro aloqalari va xavfsizlikni boshqarish usullarini qayta shakllantiruvchi muhim masalaga aylandi. Internet va raqamli texnologiyalarning tez tarqalishi muloqot va hamkorlik uchun misli ko‘rilmagan imkoniyatlarni keltirib chiqarmoqda. Biroq, bu o‘lish sezilarli zaifliklar va xavflarni ochib berdi, bu esa davlatlarni kiber tahdidlarga tobora ko‘proq moyil qilib qo‘ydi. Kiberhujumlar muhim infratuzilmalarni nishonga olishi, jamoatchilik fikrini manipulyatsiya qilishi va milliy xavfsizlikka putur etkazishi mumkin, bu esa davlatlarni diplomatiya va xalqaro mojarolarda o‘z strategiyalarini qayta ko‘rib chiqishga undaydi. Ushbu maqolada bir paytlar muhim muammo sifatida qaralgan kiberxavfsizlik bugungi kunda butun dunyo bo‘ylab milliy xavfsizlik strategiyalarining markaziy tarkibiy qismiga aylangani o‘rganiladi. Hukumatlar xakerlik, josuslik va to‘lov va qimor dasturlari kabi ortib borayotgan kibertahdidlarga diplomatiya, razvedka ma’lumotlarini almashish va xalqaro hamkorlikda yangi yondashuvlarni ishlab chiqish orqali javob bermoqda. Kiberxavfsizlik muammolarining murakkabligi davlatlardan milliy manfaatlar va global hamkorlikni muvozanatlashtiradigan keng qamrovli strategiyalarni qabul qilishni talab qiladi. Bundan tashqari, raqamli inqilob xalqaro munosabatlar manzarasini tubdan o‘zgartirib, ziddiyat va hamkorlik uchun yangi maydonlarni taqdim etadi. Ushbu maqola global quvvat dinamikasini shakllantirishda kiberxavfsizlikning o‘zgaruvchan roli va kiberxavflarni samarali boshqarish uchun xalqaro tuzilmalar va kelishuvlarga bo‘lgan ehtiyoj ortib borayotganini o‘rganadi. Siyosatchilar va olimlar kiberxavfsizlikning nozik tomonlarini tushunib, raqamli asr qo‘yayotgan muammolarni yaxshiroq hal qilishlari va xalqaro munosabatlarda barqarorlikni ta’minlashlari mumkin. Ushbu tadqiqot kiberxavfsizlik muammolari global diplomatiya va nizolarni boshqarish kelajagiga qanday ta’sir qilishini tushunish uchun qimmatli manba bo‘lib xizmat qiladi.

Kalit so‘zlar. Kiberxavfsizlik, diplomatiya, razvedka, raqamli inqilob, kiberxavflar, xakerlik, kiberfaoliyat, xalqaro munosabatlar.

THE PROBLEM OF CYBER SECURITY IN MODERN INTERNATIONAL RELATIONS

Mohigul Rahmanovna Mayusupova

*2nd year Master student in “International Relations and World Politics”,
Tashkent State University of Oriental Studies
E-mail: mohigulmayusupova@gmail.com*

Annotation: *In the digital era, cyber security has become an important issue in international relations, reshaping the way people interact and manage security. The rapid spread of the Internet and digital technologies is creating unprecedented opportunities for communication and collaboration. However, this growth has exposed significant vulnerabilities and risks, making countries increasingly vulnerable to cyber threats. Cyber attacks can target critical infrastructure, manipulate public opinion, and undermine national security, prompting states to rethink their strategies in diplomacy and international conflict. This article explores how cyber security, once viewed as a critical issue, has now become a central component of national security strategies around the world. Governments are responding to growing cyber threats, such as hacking, espionage, and ransomware, by developing new approaches to diplomacy, intelligence sharing, and international cooperation. The complexity of cyber security challenges requires states to adopt comprehensive strategies that balance national interests and global cooperation. In addition, the digital revolution will fundamentally change the landscape of international relations, providing new arenas for conflict and cooperation. This article examines the changing role of cyber security in shaping global power dynamics and the growing need for international structures and agreements to effectively manage cyber threats. By understanding the intricacies of cyber security, politicians and scientists can better address the challenges posed by the digital age and ensure stability in international relations. This research provides a valuable resource for understanding how cybersecurity challenges will affect the future of global diplomacy and conflict management.*

Keywords. *Cyber security, diplomacy, intelligence, digital revolution, cyber threats, hacking, cyber activity, international relations.*

ПРОБЛЕМА КИБЕРБЕЗОПАСНОСТИ В СОВРЕМЕННЫХ МЕЖДУНАРОДНЫХ ОТНОШЕНИЯХ

Мохигул Рахмановна Маюсупова

Студент 2 курса магистратуры по специальности «Международные
отношения и мировая политика»,
Ташкентский государственный университет востоковедения
E-mail: mohigulmayusupova@gmail.com

Аннотация: В цифровую эпоху кибербезопасность стала важной проблемой в международных отношениях, меняя способы взаимодействия людей и управления безопасностью. Быстрое распространение Интернета и цифровых технологий создает беспрецедентные возможности для общения и сотрудничества. Однако этот рост выявил значительные уязвимости и риски, что сделало страны все более уязвимыми для киберугроз. Кибератаки могут быть нацелены на критически важную инфраструктуру, манипулировать общественным мнением и подрывать национальную безопасность, побуждая государства переосмысливать свои стратегии в дипломатии и международных конфликтах. В этой статье рассматривается, как кибербезопасность, когда-то считавшаяся критической проблемой, теперь стала центральным компонентом стратегий национальной безопасности во всем мире. Правительства реагируют на растущие киберугрозы, такие как хакерство, шпионаж и программы-вымогатели, разрабатывая новые подходы к дипломатии, обмену разведанными и международному сотрудничеству. Сложность проблем кибербезопасности требует от государств принятия комплексных стратегий, которые уравнивают национальные интересы и глобальное сотрудничество. Кроме того, цифровая революция фундаментально изменит ландшафт международных отношений, предоставив новые арены для конфликтов и сотрудничества. В этой статье рассматривается меняющаяся роль кибербезопасности в формировании глобальной динамики сил и растущая потребность в международных структурах и соглашениях для эффективного управления киберугрозами. Понимая тонкости кибербезопасности, политики и ученые смогут лучше решать проблемы, возникающие в эпоху цифровых технологий, и обеспечивать стабильность в международных отношениях. Это исследование предоставляет ценный ресурс для понимания того, как проблемы кибербезопасности повлияют на будущее глобальной дипломатии и управления конфликтами.

Ключевые слова. Кибербезопасность, дипломатия, разведка, цифровая революция, киберугрозы, хакерство, киберактивность, международные отношения.

KIRISH.

Raqamli asrda kiberxavfsizlik xalqaro munosabatlarga ta'sir qiluvchi muhim masala sifatida paydo bo'ldi. Internet va raqamli texnologiyalarning keng tarqalishi

muloqot va hamkorlik uchun misli ko'rilmagan imkoniyatlarni yaratdi. Biroq, u muhim zaifliklarni ham keltirib chiqardi, bu esa davlatlarni kibertahdidlarga ko'proq moyil qiladi. Kiberxavfsizlik hodisalari muhim infratuzilmani buzishi, jamoatchilik fikrini manipulyatsiya qilishi va milliy xavfsizlikka putur etkazishi mumkin, bu esa davlatlarni diplomatiya va mojaroga yondashuvlarini qayta ko'rib chiqishga undaydi. Raqamli inqilob xalqaro munosabatlar manzarasini tubdan o'zgartirib, mojaro va hamkorlik uchun yangi maydonlarni yaratdi. Kiberxavfsizlik, bir vaqtlar o'ziga xos muammo deb hisoblangan, endi butun dunyo mamlakatlari uchun milliy xavfsizlik strategiyalarining muhim tarkibiy qismi sifatida paydo bo'ldi. Kiber tahdidlarning kuchayishi, jumladan, xakerlik, josuslik va to'lov dasturlari hukumatlarni xavfsizlik va diplomatiyaga yondashuvlarini qayta ko'rib chiqishga undadi. Shu nuqtai nazardan, kiberxavfsizlikning murakkabliklarini tushunish xalqaro munosabatlarni samarali boshqarish uchun zarurdir.

USLUBLAR.

Ushbu maqola ilmiy adabiyotlar, hukumat hisobotlari va e'tiborga molik kiber hodisalarning amaliy tadqiqotlari kabi turli manbalarga asoslangan sifatli tadqiqot metodologiyasidan foydalanadi. Xalqaro munosabatlarga taalluqli kiberxavfsizlik sohasidagi asosiy tendensiyalar va muammolarni aniqlash uchun tematik tahlil o'tkaziladi. Davlat tomonidan homiylik qilinadigan va nodavlat kiberfaoliyatlarni o'rganib, tadqiqot muammoni har tomonlama tushunishga intiladi.

NATIJALAR.

Davlat tomonidan homiylik qilinadigan kiberhujumlar strategik ustunlikka intilayotgan mamlakatlar uchun odatiy taktikaga aylandi. Diqqatga sazovor misollar orasida Rossiyaning Ukrainaga qarshi kiber operatsiyalari 2015 yilda boshlangan va 2022 yilda keng ko'lamli harbiy yurishi mobaynida avj oldi. (Brenner, S. W. 2010) Bu hujumlar elektr tarmoqlari va moliyaviy tizimlar kabi muhim infratuzilmani nishonga olgan bo'lib, kiber imkoniyatlar qanday qilib mamlakat faoliyatini buzishi va geosiyosiy mojarolarda bosim o'tkazishi mumkinligini ko'rsatib beradi. Bunday

harakatlar barqarorlikka salbiy ta’sir ko’rsatib hatto, daxshatli oqibatlarga olib kelishi mumkin. Buning ortidan ushbu harakatlar, boshqa davlatlarni kibermudofaasini va harbiy harakatlarni kuchaytirishga undaydi. (Andrew E. Kramer. 2022).

Kiberhujumlarni muayyan ishtirokchilarga bog’lash yoki asl aybdorlarni va sababchilarni topish xalqaro munosabatlarda muhim muammo bo’lib qolmoqda. Internetning o’ziga xos anonimligi ko’pincha hujumning kelib chiqish sababchisini aniqlashni qiyinlashtiradi, bu esa noaniqlik va potentsial noto’g’ri ma’lumotlarga olib keladi. Misol uchun, 2017 yilda WannaCry to’lov dasturi hujumi butun dunyo bo’ylab yuz minglab kompyuterlarga ta’sir ko’rsatdi. Hujum uchun Shimoliy Koreya ayblangan bo’lsa-da, aniq dalillarning yo’qligi kibermakondagi atributning qanchalik murakkab ekanligini ko’rsatib berdi. Bu noaniqlik davlatlar o’rtasidagi ziddiyatni kuchaytirishi mumkin, chunki davlatlar aniq va asosli bo’lmagan ma’lumotlarga tayangan holda tahdidlarga qarshi boshqa bir davlatga javob qaytarishlari mumkin.

Kiberjosuslik yana bir dolzarb muammo bo’lib, davlatlar boshqa davlatlardan maxfiy ma’lumotlarni yig’ish uchun noqonuniy faoliyat bilan shug’ullanadi. 2015-yilda xitoylik xakerlar tomonidan AQSh Kadrlar Boshqaruv Bo’limi tizimiga buzib kirishi natijasida 20 milliondan ortiq shaxslarning shaxsiy ma’lumotlarini o’g’irlanganligi ahamiyatli voqealardan biridir. Bu voqea nafaqat AQSh kiberxavfsizligining zaif tomonlarini namoyish etdi, balki AQSh-Xitoy munosabatlarini keskinlashtirdi, chunki bu kabi josuslik faoliyati davlatlar o’rtasida ishonchsizlik kayfiyatini keskin oshiradi va turli xil nizolarni keltirib chiqarishga asos bo’la oladi. (Schmidt, M. S., & Sanger, D. E. 2016).

Kiber tahdidlarning iqtisodiy oqibatlari jiddiy bo’lib, global bozorlar va savdo munosabatlariga ta’sir qiladi. Yirik korporatsiyalarga kiberhujumlar moliyaviy yo’qotishlar va nufuziga putur yetkazishi mumkin. Masalan, rossiyalik xakerlar tomonidan sodir etilgan 2020 yildagi SolarWinds kiberhujumi AQShning ko’plab davlat idoralari va xususiy kompaniyalariga kirib bordi, bu esa milliardlab zarar xarajatlarni qoplashga olib keldi va AQSh kiberxavfsizligiga nisbatan ishonchni

yo‘qotdi. Bunday hodisalar xalqaro ishbilarmonlik aloqalarini buzishi va mamlakatlarning xavfsizlikka oid xavf-xatarlar tufayli o‘zaro hamkorlikni qayta ko‘rib chiqilishiga sabab bo‘ladi.

Kiberxavfsizlik bo‘yicha yaxlit xalqaro asosning yo‘qligi ushbu muammolarni hal qilish bo‘yicha global sa’y-harakatlarni murakkablashtiradi. Kiberjinoyatlar bo‘yicha Budapesht konvensiyasi kabi tashabbuslar mavjud bo‘lsa-da, ko‘plab mamlakatlar hali kiber faoliyatni tartibga soluvchi keng qamrovli qoidalarni qabul qilmagan. Ushbu konsensusning yo‘qligi samarali hamkorlikka to‘sqinlik qiladigan kiberxavfsizlikka turlicha yondashuvlarga olib kelishi mumkin. Birlashgan Millatlar Tashkiloti kabi forumlarda kibermakonda davlat xatti-harakati normalarini o‘rnatish bo‘yicha davom etayotgan munozaralar ushbu masalalar bo‘yicha xalqaro konsensusga erishish qanchalik murakkabligini ko‘rsatadi. Kibermakonda nodavlat aktorlar, jumladan xakerlar va kiberjinoyatchilarning ko‘payishi kiberxavfsizlik muammolariga yana bir murakkablik qatlamini ko‘paytirdi. Anonim guruhlar hukumat faoliyatiga xalaqit berib, jamoatchilik fikrini o‘zgartirishi mumkin bo‘lgan siyosiy motivli hujumlar uyushtirmoqda.

Kiberxavfsizlik, shuningdek, axborot urushi bilan kesishadi, bu yerda davlatlar jamoatchilik fikri va siyosiy natijalarga ta’sir qilish uchun axborotni manipulyatsiya qiladi. Rossiyaning 2016 yilgi AQSh prezidentlik saylovlariga ijtimoiy tarmoqlardagi dezinformatsion uyushmalar orqali aralashuvi bu tendensiyaga misoldir. Bunday harakatlar demokratik jarayonlarga putur yetkazishi va jamiyatlar ichida bo‘linishlarni keltirib chiqarishi mumkin, bu esa davlatlarni kiberxavfsizlik strategiyalari va kiberhujumlarga nisbatan qarshi choralarda yanada tajovuzkor pozitsiyalarni egallashga undaydi. (Zetter, K. 2014)

Xalqaro tashkilotlar kiberxavfsizlik muammolarini bartaraf etishda hal qiluvchi rol o‘ynaydi, ammo ularning samaradorligi turlicha. Birlashgan Millatlar Tashkiloti va NATO kabi tashkilotlar a’zo davlatlar o‘rtasida kiberxavfsizlik bo‘yicha hamkorlikni rivojlantirishga qaratilgan muloqot va tamoyillarni ishlab chiqishmoqda. Biroq, milliy

manfaatlar va imkoniyatlardagi tafovutlar jamoaviy harakatlarga va hamkorlikka to’sqinlik qilishi mumkin va bu tashkilotlarning xavfsiz kiber muhitni yaratishdagi ta’sirini bir muncha cheklaydi.

Davlatlar kiberxavfsizlik masalalarini milliy xavfsizlik strategiyalariga tobora ko‘proq kiritib, uni umumiy xavfsizlikning muhim tarkibiy qismi sifatida e’tirof etmoqda. Masalan, AQSh Ichki xavfsizlik departamentining Kiberxavfsizlik va infratuzilma xavfsizligi agentligi (Cybersecurity and Infrastructure Security Agency CISA) mamlakatning muhim infratuzilmasini kibertahdidlardan himoya qilishga e’tibor qaratadi. Ushbu integratsiya kibertahdidlar milliy xavfsizlikka putur yetkazishi va risklarni boshqarishga aniq yondashuvni talab etishi ortib borayotganligini aks ettiradi.

Kiberdiplomatiyaning tadqiqot va amaliyot sohasi sifatida paydo bo‘lishi kiberxavfsizlik muammolarini hal qilish uchun diplomatik sa’y-harakatlarning ahamiyati ortib borayotganini ko‘rsatadi. Mamlakatlar hamkorlikni kuchaytirish va normalarni o‘rnatish uchun ikki va ko‘p tomonlama muloqotlarga kirisha boshladi. Masalan, AQSh va uning ittifoqchilari Yaponiya va Avstraliya kabi davlatlar bilan kiberxavfsizlik bo‘yicha jamoaviy barqarorlikni kuchaytirish uchun muzokaralar olib borishdi. Bunday sa’y-harakatlar o‘zaro ishonchni mustahkamlash va kiber nizolar bilan bog‘liq xavflarni kamaytirishga qaratilgan. Davlatlar xalqaro munosabatlarga ta’sir qilish uchun yumshoq kuch vositasi sifatida kiberxavfsizlik imkoniyatlaridan tobora ko‘proq foydalanmoqda. Masalan, davlatlar rivojlanayotgan mamlakatlarga kiberxavfsizlik bo‘yicha yordam yoki tajriba taklif qilishlari mumkin, bunda ittifoqlar tuzish va ularning ta’sirini kengaytirish yo‘lidir. Ushbu yondashuv geosiyosiy dinamikaga ta’sir qiluvchi qaramlikka olib keladi. (Garry, A. 2019).

Rivojlangan va rivojlanayotgan mamlakatlar o‘rtasidagi kiberxavfsizlik imkoniyatlaridagi nomutanosiblik global kiberxavfsizlik uchun muammolarni keltirib chiqaradi. Rivojlanayotgan mamlakatlarda ko‘pincha kibertahdidlardan samarali himoya qilish uchun resurslar va infratuzilma yetishmaydi, bu esa ularni zaif

nishonlarga aylantiradi. Bu tengsizlik xalqaro munosabatlardagi mavjud kuch nomutanosibligini kuchaytirishi mumkin, chunki texnologik jihatdan rivojlangan davlatlar kam rivojlangan mintaqalardagi zaifliklardan foydalanishi mumkin. (Schmidt, M. S., & Sanger, D. E. 2016)

Jamoatchilikning kiberxavfsizlik tahdidlarini idrok etishi hukumat siyosati va xalqaro munosabatlarga ta’sir qiladi. Yuqori darajadagi kiber hodisalar ko‘pincha jamoatchilikning noroziligiga va xavfsizlik choralarini kuchaytirish talabiga olib keladi. Kiberxavfsizlik bo‘yicha malakali mutaxassislariga talab ortib borayotganligi sababli, mamlakatlar o‘zlarining kiberxavfsizlik salohiyatini oshirish uchun ta’lim va o‘quv dasturlariga sarmoya kiritmoqda. Yevropa Ittifoqining a’zo davlatlarda kiberxavfsizlik ko‘nikmalarini oshirishga qaratilgan sa’y-harakatlari kabi xalqaro hamkorlik yanada xavfsizroq global muhitni yaratishga qaratilgan. Imkoniyatlarni oshirish kiber tahdidlarga qarshi chidamlilikni oshirishga va davlatlar o‘rtasida hamkorlikni rivojlantirishga olib keladi.

MUHOKAMA.

Izlanish natijalari shuni ko‘rsatadiki, kiberxavfsizlik nafaqat texnik masala, balki xalqaro munosabatlarni chuqur tushunishni talab qiladigan geosiyosiy muammodir. Davlat tomonidan homiylik qilinadigan kiberfaoliyatlar urush haqidagi an’anaviy tushunchalarni murakkablashtirib, tashqi siyosat quroli sifatida tobora ko‘proq foydalanilmoqda. Aniq atributlash mexanizmlarining yo‘qligi keskinlikni kuchaytiradi, chunki davlatlar aniqlangan faktlarga emas, balki idrok etilgan tahdidlarga asoslanib javob beradi.

Kiberxavfsizlikning milliy suverenitetga ta’siri yana bir muhim masala. Hukumatlar kibertahdidlarga qarshi kurash bo‘yicha nazorat choralarini amalga oshirar ekan, ular xavfsizlikni ta’minlash va fuqarolar huquqlarini himoya qilish o‘rtasidagi nozik masalalarni hisobga olishi kerak. Bu muvozanatni saqlamaslik ichki tartibsizliklarga va jamoatchilik ishonchining pasayishiga olib keladi.

Shuningdek, global hamkorlik zaruriyatini ortiqcha baholab bo‘lmaydi. Kibertahdidlar tabiatan transmilliy xususiyatga ega bo‘lib, davlatlardan mustahkam mudofaa va javob strategiyalarini ishlab chiqish uchun birgalikda ishlashni talab qiladi. Axborot almashish va salohiyatni oshirish kiberxavfsizlikka kompleks yondashuvning muhim tarkibiy qismlari bo‘lib, mamlakatlarga o‘zlarining muhim infratuzilmalarini yaxshiroq himoya qilish va yuzaga kelayotgan tahdidlarga javob berish imkonini beradi.

XULOSA.

Zamonaviy xalqaro munosabatlarda kiberxavfsizlik muammosi murakkab va ko‘p qirrali muammolarni keltirib chiqaradi. Davlatlar davlat homiyligidagi kiberoperatsiyalar voqealari va atributlashtirish qiyinchiliklariga duch kelar ekan, samarali javoblarni ishlab chiqish uchun hamkorlikdagi zarur sa’y-harakatlar ko‘rishlari zarur. Kiberxavfsizlik muammolarini hal qilishda xalqaro me’yorlarni yaratish, atributlashtirish mexanizmlarini takomillashtirish va global hamkorlikni rivojlantirish muhim ahamiyatga ega bo‘ladi. Raqamli va shxasiy xavfsizlik tobora o‘zaro bog‘lanib borayotgan dunyoda barqaror va xavfsiz kiber muhitga intilish nafaqat milliy tashvish, balki global talabdir. Taraqqiy etishda davlatlar barcha uchun bexatar va xavfsiz kelajakni ta’minlash uchun xalqaro munosabatlar kun tartibida kiberxavfsizlikni birinchi o‘ringa qo‘yishlari kerak.

FOYDALANILGAN ADABIYOTLAR.

1. Andrew E. Kramer. (2022). For an overview of Russia’s cyber operations against Ukraine, “Russia's Cyberattacks on Ukraine,”The New York Times, March 2022.
2. Brenner, S. W. (2010). Cyber Threats: The New Normal in International Relations. Harvard International Review, 31(1), 10-15.
3. Garry, A. (2019). Cybersecurity and International Relations: The New Frontier. International Security, 44(2), 45-76.
4. Nye, J. S. (2010). Cyber Power. Harvard University Press. pp. 1-150.
5. Roth, C. (2015). The Role of International Law in Cyber Security. Journal of Cybersecurit, 1(1), 23-35.

6. Schmidt, M. S., & Sanger, D. E. (2016). U.S. Accuses Russia of Cyberattacks. The New York Times. Retrieved from [NY Times] (<https://www.nytimes.com>).
7. Tamm, H. (2016). The Importance of Attribution in Cybersecurity. International Journal of Information Security, 15(2), 133-145.
8. Zetter, K. (2014). Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Crown Publishing Group. pp. 1-300.