KIBERXAVFSIZLIK: RAQAMLI JAMIYATNING ASOSIY HIMOYA VOSITASI

Xorazm viloyat Hazorasp tumani 1-son Texnikumida informatika fan o‘qtuvchisi

Otaniyozova Zaynabxon Shoripboyevna

ANNOTATSIYA

Mazkur maqolada raqamli jamiyat sharoitida kiberxavfsizlikning tutgan o‘rni, uning davlat, biznes va fuqarolar faoliyatidagi ahamiyati tahlil qilingan. Axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi natijasida raqamli xizmatlar soni ortib borayotgan bir paytda kiberxavfsizlik masalalari ham dolzarb tus olmoqda. Tadqiqot davomida kiberhujumlarning asosiy turlari, ularning iqtisodiy va ijtimoiy oqibatlari hamda ularga qarshi kurashish mexanizmlari o‘rganildi. O‘zbekiston Respublikasida kiberxavfsizlikni ta’minlash bo‘yicha amalga oshirilayotgan islohotlar, normativ-huquqiy asoslar va amaliy choralar tahlil qilindi. Tadqiqot natijalari shuni ko‘rsatdiki, zamonaviy raqamli infratuzilmaning barqaror faoliyat yuritishi nafaqat texnik vositalar, balki foydalanuvchilarning axborot madaniyati va kiberxavfsizlik bo‘yicha bilim darajasiga ham bog‘liq. Shuningdek, davlat organlari, xususiy sektor va ta’lim muassasalari o‘rtasidagi hamkorlik kiberxavfsizlik tizimining samaradorligini oshirishda muhim omil hisoblanadi.

Kalit so‘zlar: Kiberxavfsizlik, raqamli jamiyat, axborot xavfsizligi, kiberhujum, ma’lumotlarni himoyalash, raqamli transformatsiya, kiberjinoyatchilik, axborot texnologiyalari, kiberxatarlar, shaxsiy ma’lumotlar.

КИБЕРБЕЗОПАСНОСТЬ: ОСНОВНОЙ ИНСТРУМЕНТ ЗАЩИТЫ ЦИФРОВОГО ОБЩЕСТВА

АННОТАЦИЯ

В данной статье анализируется роль кибербезопасности в цифровом обществе, ее значение для деятельности государства, бизнеса и граждан. По мере роста числа цифровых услуг в результате стремительного развития информационно-коммуникационных технологий, вопросы кибербезопасности также приобретают все большее значение. В ходе исследования были изучены основные виды кибератак, их экономические и социальные последствия, а также механизмы борьбы с ними. Проанализированы реформы, нормативно-правовая база и практические меры, реализуемые для обеспечения кибербезопасности в Республике Узбекистан. Результаты исследования показали, что стабильное функционирование современной цифровой инфраструктуры зависит не только от технических средств, но и от уровня информационной культуры и знаний пользователей в области кибербезопасности. Также важным фактором повышения эффективности системы кибербезопасности является сотрудничество между государственными органами, частным сектором и образовательными учреждениями.

Ключевые слова: Кибербезопасность, цифровое общество, информационная безопасность, кибератака, защита данных, цифровая трансформация, киберпреступность, информационные технологии, киберугрозы, персональные данные.

CYBERSECURITY: THE MAIN PROTECTION TOOL OF THE DIGITAL SOCIETY

ABSTRACT

This article analyzes the role of cybersecurity in the digital society, its importance in the activities of the state, business and citizens. As the number of digital services increases as a result of the rapid development of information and communication technologies, cybersecurity issues are also becoming relevant. During the study, the main types of cyberattacks, their economic and social consequences, and mechanisms for combating them were studied. The reforms, regulatory and legal frameworks and practical measures being implemented to ensure cybersecurity in the Republic of Uzbekistan were analyzed. The results of the study showed that the stable operation of modern digital infrastructure depends not only on technical means, but also on the level of information culture and cybersecurity knowledge of users. Also, cooperation between government bodies, the private sector and educational institutions is an important factor in increasing the effectiveness of the cybersecurity system.

Keywords: Cybersecurity, digital society, information security, cyberattack, data protection, digital transformation, cybercrime, information technology, cyberthreats, personal data.

KIRISH

XXI asrda axborot texnologiyalarining rivojlanishi insoniyat hayotining deyarli barcha sohalarini qamrab oldi. Davlat boshqaruvi, bank tizimi, ta’lim, sog‘liqni saqlash, transport va savdo kabi yo‘nalishlarda raqamli texnologiyalar keng joriy etilmoqda. Natijada ma’lumotlar hajmi keskin ortib, ularni saqlash va qayta ishlash jarayonlari murakkablashmoqda. Shu bilan birga, axborot tizimlariga nisbatan noqonuniy kirish, ma’lumotlarni o‘g‘irlash, zararli dasturlar orqali tizimlarga zarar yetkazish kabi xavf-xatarlar ham ko‘paymoqda.

O‘zbekiston Respublikasida ham so‘nggi yillarda raqamli iqtisodiyot va elektron hukumat tizimini rivojlantirish bo‘yicha keng ko‘lamli ishlar amalga oshirilmoqda. “Raqamli O‘zbekiston – 2030” strategiyasining qabul qilinishi mamlakatning raqamli taraqqiyot yo‘nalishidagi muhim qadamlardan biri bo‘ldi. Raqamli xizmatlar sonining ortishi esa axborot xavfsizligi va kiberxavfsizlikni mustahkamlash zaruratini yanada kuchaytirdi. Chunki har qanday raqamli tizimning ishonchliligi uning himoyalanganlik darajasi bilan belgilanadi.

Bugungi kunda dunyo bo‘ylab amalga oshirilayotgan kiberhujumlar davlatlarning iqtisodiy xavfsizligiga, korxonalarning moliyaviy faoliyatiga va fuqarolarning shaxsiy hayotiga jiddiy zarar yetkazmoqda. Shu sababli kiberxavfsizlik masalasi faqat texnik muammo emas, balki milliy xavfsizlikning muhim tarkibiy qismi sifatida qaralmoqda. Mazkur tadqiqotning dolzarbligi ham aynan raqamli jamiyatda kiberxavfsizlikning ahamiyatini chuqur o‘rganish zarurati bilan izohlanadi.

METODOLOGIYA

Tadqiqot jarayonida ilmiy bilishning bir qator zamonaviy usullaridan foydalanildi. Avvalo, mavzuga oid ilmiy adabiyotlar, xalqaro tashkilotlar hisobotlari, normativ-huquqiy hujjatlar va statistik ma’lumotlar tahlil qilindi. Qiyosiy tahlil usuli yordamida rivojlangan davlatlarning kiberxavfsizlik bo‘yicha tajribalari O‘zbekiston amaliyoti bilan solishtirildi.

Shuningdek, tizimli yondashuv asosida kiberxavfsizlikning texnik, tashkiliy va huquqiy jihatlari kompleks ravishda o‘rganildi. Analitik usul yordamida kiberxatarlarning kelib chiqish sabablari, ularning oqibatlari va oldini olish mexanizmlari baholandi. Statistik ma’lumotlarni umumlashtirish orqali kiberjinoyatchilikning rivojlanish tendensiyalari aniqlandi.

Tadqiqot davomida kuzatish, tavsiflash va ilmiy umumlashtirish usullaridan ham foydalanildi. Olingan natijalar asosida kiberxavfsizlikni rivojlantirishga qaratilgan amaliy tavsiyalar ishlab chiqildi.

NATIJALAR

Tadqiqot natijalari shuni ko‘rsatdiki, raqamli texnologiyalarning jadal rivojlanishi bilan bir qatorda kiberxatarlar soni ham ortib bormoqda. Kiberhujumlarning eng ko‘p uchraydigan turlari orasida fishing, zararli dasturlar, DDoS hujumlari, ma’lumotlarni noqonuniy qo‘lga kiritish va ijtimoiy muhandislik usullari alohida o‘rin tutadi. Ushbu tahdidlar davlat organlari, moliyaviy institutlar va xususiy kompaniyalar faoliyatiga sezilarli zarar yetkazishi mumkin. Tahlillar natijasida aniqlanishicha, kiberxavfsizlik tizimining samaradorligi nafaqat texnik vositalarga, balki inson omiliga ham bog‘liq. Ko‘plab kiberhodisalar foydalanuvchilarning axborot xavfsizligi qoidalariga yetarli darajada rioya qilmasligi oqibatida yuzaga keladi. Shu sababli aholining kiberxavfsizlik madaniyatini oshirish muhim vazifa hisoblanadi.

O‘zbekiston Respublikasida kiberxavfsizlikni mustahkamlash maqsadida qator normativ-huquqiy hujjatlar qabul qilingan. Xususan, “Kiberxavfsizlik to‘g‘risida”gi Qonun va “Raqamli O‘zbekiston – 2030” strategiyasi ushbu sohada tizimli ishlarni tashkil etish uchun muhim huquqiy asos yaratdi. Natijalar shuni ko‘rsatadiki, davlat organlari va tashkilotlarda axborot tizimlarini himoyalash darajasi yildan-yilga oshib bormoqda.

Tadqiqot yakunlari asosida kiberxavfsizlikni ta’minlashda zamonaviy himoya vositalarini joriy etish, mutaxassislar tayyorlash, foydalanuvchilar savodxonligini oshirish hamda xalqaro hamkorlikni rivojlantirish eng ustuvor yo‘nalishlar ekanligi aniqlandi. Raqamli jamiyatning barqaror rivojlanishi bevosita kiberxavfsizlik tizimining ishonchliligi va samaradorligiga bog‘liq ekanligi ilmiy jihatdan asoslandi.

MUHOKAMA

Raqamli transformatsiya jarayonlarining jadallashuvi natijasida kiberxavfsizlik masalasi zamonaviy jamiyat rivojlanishining eng muhim omillaridan biriga aylandi. Bir necha yil avval axborot xavfsizligi asosan yirik korxonalar va davlat tashkilotlari doirasida muhokama qilingan bo‘lsa, bugungi kunda u har bir

fuqaroning kundalik hayoti bilan bevosita bog‘liq bo‘lib qoldi. Elektron to‘lov tizimlari, internet-banking, elektron hukumat xizmatlari, masofaviy ta’lim platformalari va bulutli texnologiyalarning keng qo‘llanilishi foydalanuvchilar uchun katta qulaylik yaratmoqda. Shu bilan birga, ushbu tizimlar turli kiberxatarlar uchun ham nishonga aylanmoqda. Kiberjinoyatchilar tobora murakkablashib borayotgan usullardan foydalanmoqda. Avvallari oddiy viruslar orqali amalga oshirilgan hujumlar bugungi kunda sun’iy intellekt elementlari qo‘llanilgan murakkab sxemalar orqali tashkil qilinmoqda. Bu esa himoya choralarini doimiy ravishda takomillashtirib borishni talab etadi. Ayniqsa, ma’lumotlarning iqtisodiy resurs sifatidagi ahamiyati ortib borayotgani ularni himoya qilish zaruratini yanada kuchaytirmoqda. Mutaxassislarning fikricha, kelajakda ma’lumotlar strategik resurs sifatida energiya yoki tabiiy boyliklar qatorida baholanishi mumkin. Shunday ekan, kiberxavfsizlikni faqat texnik masala sifatida emas, balki iqtisodiy va ijtimoiy taraqqiyotning muhim tarkibiy qismi sifatida ko‘rib chiqish lozim.

Tahlillar shuni ko‘rsatadiki, kiberhujumlarning asosiy qismi inson omili bilan bog‘liq. Ko‘plab foydalanuvchilar oddiy xavfsizlik qoidalariga rioya qilmaydi, murakkab bo‘lmagan parollardan foydalanadi yoki noma’lum havolalarga kiradi. Natijada axborot tizimlariga noqonuniy kirish holatlari yuzaga keladi. Ba’zan eng zamonaviy texnik himoya vositalari ham foydalanuvchining ehtiyotsizligi sababli samarasiz bo‘lib qoladi. Shu nuqtai nazardan qaralganda, kiberxavfsizlik madaniyatini shakllantirish texnik vositalarni joriy qilishdan kam ahamiyatga ega emas. Raqamli savodxonlik darajasi yuqori bo‘lgan jamiyatlarda kiberjinoyatchilik oqibatlari nisbatan kam kuzatiladi. Ta’lim muassasalarida axborot xavfsizligi bo‘yicha maxsus kurslarni joriy etish, aholiga muntazam tushuntirish ishlarini olib borish va amaliy mashg‘ulotlar tashkil etish muhim natija berishi mumkin. Bugungi kunda yoshlar internetdan eng faol foydalanuvchilar hisoblanadi. Shu sababli aynan yosh avlod orasida kibergigiyena ko‘nikmalarini shakllantirish dolzarb vazifa sanaladi.

O‘zbekiston Respublikasida raqamlashtirish jarayonlari keng ko‘lamda amalga oshirilmoqda. Elektron davlat xizmatlari sonining ortishi fuqarolar uchun qulaylik yaratmoqda. Davlat xizmatlarining elektron shaklga o‘tkazilishi natijasida vaqt va mablag‘ tejalmoqda. Lekin xizmatlar soni oshgan sari ularga qaratilgan kiberxatarlar ham ko‘paymoqda. Elektron ma’lumotlar bazalarida millionlab foydalanuvchilarning shaxsiy ma’lumotlari saqlanadi. Mazkur ma’lumotlarning sizib chiqishi nafaqat iqtisodiy zarar, balki fuqarolarning konstitutsiyaviy huquqlariga ham putur yetkazishi mumkin. Shu sababli davlat axborot tizimlarini himoyalash strategik ahamiyatga ega. O‘zbekistonning so‘nggi yillardagi tajribasi ko‘rsatmoqdaki, kiberxavfsizlik bo‘yicha maxsus markazlar tashkil etilishi va normativ-huquqiy bazaning takomillashuvi ijobiy natijalar bermoqda. Shunga qaramasdan, texnologiyalar rivojlanishi bilan yangi tahdidlar ham paydo bo‘lib bormoqda. Kiberxavfsizlikning iqtisodiy jihati ham alohida e’tiborga loyiqdir. Jahon miqyosida kiberjinoyatlar natijasida yuzaga keladigan zarar har yili milliardlab dollarni tashkil etmoqda. Kompaniyalar ma’lumotlar bazasining buzilishi sababli nafaqat moliyaviy yo‘qotishlarga, balki obro‘-e’tiborining pasayishiga ham duch kelmoqda. Ayrim hollarda mijozlarning ishonchini tiklash uchun yillar talab etiladi. Ayniqsa, bank va moliya sektoridagi kiberhodisalar iqtisodiyot barqarorligiga sezilarli ta’sir ko‘rsatadi. Shu bois korxonalar axborot xavfsizligini xarajat emas, balki investitsiya sifatida baholashi zarur. Amaliyot shuni ko‘rsatadiki, profilaktika tadbirlariga sarflangan mablag‘ keyinchalik yuzaga kelishi mumkin bo‘lgan zarar miqdoridan bir necha barobar kam bo‘ladi.

Kiberxavfsizlikning yana bir muhim yo‘nalishi shaxsiy ma’lumotlarni himoyalash bilan bog‘liq. Zamonaviy foydalanuvchi kundalik faoliyati davomida juda katta hajmdagi ma’lumotlarni internet tizimlariga taqdim etadi. Telefon raqamlari, bank kartalari rekvizitlari, biometrik ma’lumotlar va elektron pochta manzillari turli platformalarda saqlanadi. Ushbu ma’lumotlar noqonuniy qo‘lga kiritilgan taqdirda, firibgarlik holatlari yuzaga kelishi mumkin. Shuning uchun

ma’lumotlarni himoyalash nafaqat davlatning, balki har bir foydalanuvchining ham mas’uliyatini talab qiladi. Murakkab parollardan foydalanish, ikki bosqichli autentifikatsiyani yoqish va dasturiy ta’minotni muntazam yangilab borish eng oddiy, ammo samarali himoya vositalari hisoblanadi.

Jadval 1. Kiberxavfsizlik tahdidlari va ularning oqibatlari

Tahdid turi	**Tavsifi**	**Mumkin bo‘lgan oqibatlar**
Fishing	Soxta xabar yoki sayt orqali ma’lumotlarni qo‘lga kiritish	Shaxsiy ma’lumotlar o‘g‘irlanishi
Viruslar	Tizimga zarar yetkazuvchi dasturlar	Ma’lumotlarning yo‘qolishi
DDoS hujumlari	Serverlarga ortiqcha yuklama berish	Xizmatlarning to‘xtashi
Ransomware	Ma’lumotlarni shifrlab to‘lov talab qilish	Moliyaviy zarar
Ijtimoiy muhandislik	Psixologik usullar orqali aldash	Maxfiy ma’lumotlarning oshkor bo‘lishi

Tahlillar natijasi shuni ko‘rsatadiki, kiberxavfsizlikni ta’minlashda xalqaro hamkorlik muhim rol o‘ynaydi. Kiberjinoyatlar ko‘pincha transmilliy xarakterga ega bo‘lib, bir mamlakat hududida turib boshqa davlat axborot tizimlariga hujum uyushtirilishi mumkin. Shu sababli davlatlar o‘rtasida axborot almashinuvi va qo‘shma dasturlarni amalga oshirish muhim ahamiyat kasb etadi. Xalqaro tashkilotlar tomonidan ishlab chiqilgan standartlar va tavsiyalar milliy xavfsizlik tizimlarini takomillashtirishda foydali manba hisoblanadi. O‘zbekistonning ham xalqaro hamkorlikni kengaytirishi kiberxavfsizlik sohasida ilg‘or tajribalarni o‘zlashtirish imkonini beradi.

XULOSA

O‘tkazilgan tadqiqot natijalari kiberxavfsizlikning zamonaviy raqamli jamiyatning ajralmas qismi ekanligini ko‘rsatdi. Raqamli texnologiyalar hayotimizning barcha sohalariga chuqur kirib borar ekan, axborot tizimlarini himoyalash masalasi yanada dolzarb tus olmoqda. Kiberxatarlarning ko‘payishi davlat organlari, biznes subyektlari va fuqarolardan yangi yondashuvlarni talab etmoqda. Tadqiqot davomida kiberhujumlarning asosiy turlari, ularning oqibatlari va oldini olish mexanizmlari tahlil qilindi.

Olingan natijalar shuni tasdiqladiki, kiberxavfsizlik faqat texnik vositalar bilan cheklanmaydi. Inson omili, axborot madaniyati va raqamli savodxonlik darajasi ham muhim ahamiyatga ega. Davlat tomonidan qabul qilinayotgan dasturlar va qonunchilik hujjatlari ushbu sohani rivojlantirish uchun mustahkam asos yaratmoqda. Kelgusida zamonaviy himoya texnologiyalarini keng joriy etish, malakali mutaxassislar tayyorlash va xalqaro hamkorlikni rivojlantirish kiberxavfsizlik tizimining samaradorligini yanada oshirishga xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR

1. O‘zbekiston Respublikasi Prezidentining 2020-yil 5-oktabrdagi PF–6079-son Farmoni. Raqamli O‘zbekiston – 2030 strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risida. – Toshkent, 2020. – 52 b.
2. O‘zbekiston Respublikasi Prezidentining 2023-yil 11-sentabrdagi PF–158-son Farmoni. O‘zbekiston – 2030 strategiyasi to‘g‘risida. – Toshkent, 2023. – 48 b.
3. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni. – Toshkent: Adolat, 2022. – 24 b.
4. O‘zbekiston Respublikasining “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni. – Toshkent: Adolat, 2019. – 18 b.
5. O‘zbekiston Respublikasi Raqamli texnologiyalar vazirligi. Raqamli iqtisodiyot va elektron hukumatni rivojlantirish bo‘yicha rasmiy materiallar. – Toshkent,

2024. – 86 b.

6. ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements. – Geneva: International Organization for Standardization, 2022. – 34 p.
7. Stallings W. Cryptography and Network Security: Principles and Practice. – 8th ed. – New York: Pearson Education, 2023. – 880 p.
8. Schneier B. Applied Cryptography: Protocols, Algorithms and Source Code in C. – 20th Anniversary Edition. – New York: John Wiley & Sons, 2015. – 784 p.
9. Kaspersky Security Bulletin 2024. Cybersecurity Trends and Statistics Report. – Moscow: Kaspersky Lab, 2024. – 112 p.
10. Cisco Systems. Cisco Cybersecurity Readiness Index 2024. – San Jose: Cisco, 2024. – 76 p.
11. NortonLifeLock. Cyber Safety Insights Report 2024. – Tempe: NortonLifeLock Inc., 2024. – 58 p.
12. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2024. – Athens: ENISA, 2024. – 145 p.
13. World Economic Forum. Global Cybersecurity Outlook 2024. – Geneva: WEF, 2024. – 88 p.
14. International Telecommunication Union (ITU). Global Cybersecurity Index 2024. – Geneva: ITU, 2024. – 196 p.
15. Organisation for Economic Co-operation and Development (OECD). Digital Security Risk Management for Economic and Social Prosperity. – Paris: OECD Publishing, 2023. – 102 p.