ISSN 3060-4567

"KIBERXAVFSIZLIK: RAQAMLI DUNYODA HIMOYA MUAMMOLARI VA ECHIMLARI"

“КИБЕРБЕЗОПАСНОСТЬ: ПРОБЛЕМЫ И РЕШЕНИЯ ЗАЩИТЫ В ЦИФРОВОМ МИРЕ”

“CYBERSECURITY: CHALLENGES AND SOLUTIONS IN THE DIGITAL WORLD”

Muallif: [1]Ismatullayev Zohidbek

[2]Andijon davlat texnika instituti,

"Axborot texnologiyalari va tizimlari" yo‘nalishi, 2-kurs talabasi

*[[3]Xat yozish uchun: ✉ **Email: zohidismatullayev288@gmail.com**]*

Annotatsiya. *Ushbu maqola zamonaviy axborot texnologiyalari jadal rivojlanayotgan davrda kiberxavfsizlikning ahamiyatini yoritishga bag‘ishlangan. Bugungi raqamli dunyoda barcha sohalar – ta’lim, tibbiyot, moliya, davlat boshqaruvi va boshqa ko‘plab tizimlar axborot texnologiyalariga bevosita bog‘langan. Shu bilan birga, bu sohalar turli kiberxavf va tahdidlarga duch kelmoqda. Kiberjinoyatlar, xakerlik hujumlari, ma’lumotlar o‘g‘irlanishi, zararli dasturlar orqali tizimlarga tajovuzlar ko‘payib bormoqda. Maqolada aynan shu muammolar tahlil qilinadi, kiberxavfsizlik sohasidagi eng asosiy tahdidlar ko‘rsatib o‘tiladi va ularning jamiyat, tashkilotlar hamda oddiy foydalanuvchilarga ta’siri yoritiladi. Shuningdek, axborot himoyasini ta’minlash yo‘llari, zamonaviy himoya vositalari (antiviruslar, shifrlash texnologiyalari, ikki bosqichli autentifikatsiya va boshqalar) haqida ma’lumotlar beriladi. Maqolada kiberxavfsizlik sohasidagi global tajribalar va ilg‘or mamlakatlar misolida olib borilayotgan ishlar ham keltiriladi. Oxirida esa O‘zbekistonda kiberxavfsizlikni mustahkamlash bo‘yicha amalga oshirilayotgan chora-tadbirlar va istiqboldagi vazifalar haqida fikr yuritiladi. Ushbu maqola axborot xavfsizligi sohasiga qiziquvchi talabalar, IT mutaxassislari va raqamli muhitda xavfsiz ishlashni istagan har bir kishi uchun foydali bo‘ladi.*

ISSN 3060-4567

Kalit so‘zlar. *kiberxavfsizlik, raqamli xavfsizlik, axborot himoyasi, kiberjinoyat, xakerlik, zararli dastur, shifrlash texnologiyalari, autentifikatsiya, raqamli tahdidlar, antivirus dasturlar, axborot texnologiyalari, ma’lumotlar xavfsizligi, internet xavfsizligi, himoya tizimlari, IT xavfsizlik.*

Аннотация. *Данная статья посвящена освещению важности кибербезопасности в условиях стремительного развития современных информационных технологий. В современном цифровом мире все сферы - образование, здравоохранение, финансы, государственное управление и многие другие - непосредственно связаны с информационными системами. Однако вместе с этим возрастает и уровень угроз, связанных с киберпреступностью. Участились случаи хакерских атак, кражи данных, проникновения вредоносного программного обеспечения в системы. В статье анализируются основные проблемы в сфере кибербезопасности, приводятся типичные угрозы и их влияние на общество, организации и отдельных пользователей. Также рассматриваются способы защиты информации, в том числе современные инструменты безопасности: антивирусные программы, технологии шифрования, двухфакторная аутентификация и другие. Отдельное внимание уделено международному опыту в области кибербезопасности и приводятся примеры успешных решений в передовых странах. В заключительной части статьи рассматриваются меры, принимаемые в Узбекистане для укрепления кибербезопасности, и обозначаются приоритетные направления на будущее. Статья будет полезна студентам, интересующимся вопросами информационной безопасности, специалистам IT-сферы, а также всем, кто стремится к безопасной работе в цифровой среде.*

Ключевые слова. *кибербезопасность, цифровая безопасность, защита информации, киберпреступления, хакерские атаки, вредоносные программы, технологии шифрования, аутентификация, цифровые угрозы, антивирусные программы, информационные технологии, безопасность данных, интернет-безопасность, системы защиты, ИТ-безопасность.*

ISSN 3060-4567

Annotation. *This article is dedicated to highlighting the importance of cybersecurity in an era of rapidly developing information technologies. In today's digital world, all sectors - including education, healthcare, finance, public administration, and many others - are directly connected to information systems. However, these sectors are increasingly exposed to various cyber threats and dangers. Cybercrimes, hacking attacks, data breaches, and malware intrusions are becoming more frequent. The article analyzes these issues by identifying the main threats in the field of cybersecurity and discusses their impact on society, organizations, and individual users. It also provides an overview of methods to ensure information protection, including modern security tools such as antivirus software, encryption technologies, and two-factor authentication. Furthermore, the article explores international experiences in cybersecurity and presents examples from leading countries in this domain. It concludes by reviewing the steps being taken in Uzbekistan to strengthen cybersecurity and outlines future tasks and prospects. This article is useful for students interested in information security, IT professionals, and anyone who wants to work safely in the digital environment.*

Keywords*: cybersecurity, digital security, information protection, cybercrime, hacking, malware, encryption technologies, authentication, digital threats, antivirus software, information technologies, data security, internet safety, security systems, IT security.*

Zamonaviy axborot texnologiyalari sohasidagi jadal rivojlanish inson faoliyatining deyarli barcha jabhalariga chuqur ta'sir ko'rsatmoqda. Ta'lim tizimi, tibbiyot, moliya sektori, davlat boshqaruvi va boshqa ko'plab sohalar endi axborot texnologiyalariga bevosita bog'langan va ularning samaradorligi, tezligi va sifatini oshirishda ushbu texnologiyalar muhim ahamiyatga ega. Biroq, bu rivojlanish bilan birga kiberxavfsizlik muammolari va tahdidlari ham keskin oshib bormoqda. Raqamli dunyoda yuzaga kelayotgan yangi xavf-xatarlar, shu jumladan kiberhujumlar va ma'lumotlar o'g'irlanishi, tizimlarning ishonchliligiga salbiy ta'sir ko'rsatib, butun jamiyat va iqtisodiyot uchun jiddiy muammolarni yuzaga keltirmoqda. Shu sababli,

zamonaviy sharoitda kiberxavfsizlikni ta’minlashning ahamiyati tobora ortib bormoqda. Kiberxavfsizlikdagi asosiy muammolar va tahdidlar Bugungi kunda kiberjinoyatlar turli shakllarda namoyon bo‘lmoqda. Eng keng tarqalgan tahdidlar orasida xakerlik hujumlari, zararli dasturlar (viruslar, troyanlar, ransomware), ma’lumotlarni o‘g‘irlash, shuningdek, tizimlarga ruxsatsiz kirishlar mavjud. Ushbu tahdidlar kompaniyalar, davlat organlari, shaxsiy foydalanuvchilar va hatto global infratuzilmalar uchun xavf tug‘diradi. Masalan, moliya sektoridagi bank hisoblari buzilishi yoki shaxsiy ma’lumotlarning oshkor bo‘lishi katta moliyaviy va obro‘ zararlariga olib keladi. Shu bilan birga, ta’lim va tibbiyot sohalarida ma’lumotlar maxfiyligi va yaxlitligini ta’minlashning ahamiyati yuqori bo‘lib, u yerda yuzaga keladigan xatolik yoki hujumlar inson hayotiga bevosita tahdid solishi mumkin. Bu muammolarni chuqur tahlil qilish va ularni oldini olish uchun samarali choralar ko‘rish zarurati mavjud. Kiberxavfsizlikni ta’minlash vositalari va usullari Kiberxavfsizlikni ta’minlash uchun zamonaviy texnologiyalar va vositalar muhim rol o‘ynaydi. Antivirus dasturlari zararli dasturlarni aniqlash va yo‘q qilishda asosiy himoya choralari hisoblanadi. Shifrlash texnologiyalari ma’lumotlarni xavfsiz saqlash va uzatishda muhim ahamiyatga ega bo‘lib, ularni ruxsatsiz shaxslardan himoya qiladi. Ikki bosqichli autentifikatsiya (2FA) esa foydalanuvchilarning tizimlarga kirishini yanada mustahkamlaydi, chunki u faqat parolga emas, balki qo‘shimcha tasdiqlash usuliga ham tayanadi. Shuningdek, xavfsizlik devorlari (firewalls), zararli trafikni aniqlovchi tizimlar (IDS/IPS), va zamonaviy monitoring vositalari orqali tarmoq xavfsizligi ta’minlanadi. Ma’lumotlarni zaxiralash (backup) ham kiberhujumlardan keyin tizimlarni tiklash imkonini beradi. Shu bilan birga, kiberxavfsizlik sohasida inson omili ham muhim bo‘lib, foydalanuvchilarning xavfsizlik qoidalariga rioya qilishi ham zarur. Global tajribalar va ilg‘or mamlakatlar yondashuvlari Dunyoda ilg‘or mamlakatlar kiberxavfsizlik sohasida keng qamrovli chora-tadbirlarni amalga oshirmoqda. Ular maxsus kiberxavfsizlik markazlarini tashkil etib, hukumat, xususiy sektor va ilmiy sohalar o‘rtasida hamkorlikni rivojlantirmoqda. Masalan, AQShda NIST (National Institute of Standards and Technology) tomonidan ishlab chiqilgan kiberxavfsizlik standartlari ko‘plab davlatlar

uchun namuna hisoblanadi. Yevropa Ittifoqi esa GDPR kabi ma’lumotlarni himoya qilish qonunlari orqali kiberxavfsizlikni tartibga solmoqda. Shuningdek, Isroil, Singapur va Janubiy Koreya kabi davlatlar yuqori texnologiyalar asosida kiberxavfsizlikni rivojlantirishda yetakchi o‘rinlarni egallaydi. Ushbu mamlakatlar tajribalaridan o‘rganish va ularni O‘zbekistonga moslashtirish kiberxavfsizlikni yanada mustahkamlashda muhim ahamiyatga ega. O‘zbekistonda kiberxavfsizlikning hozirgi holati va istiqboli.O‘zbekistonda so‘nggi yillarda kiberxavfsizlikni rivojlantirish borasida sezilarli ishlar amalga oshirilmoqda. Davlat darajasida maxsus qonunlar qabul qilinib, kiber. xavfsizlikni ta’minlashga qaratilgan strategiyalar ishlab chiqilmoqda. Shuningdek, axborot texnologiyalari sohasida malakali kadrlarni tayyorlash va ularning malakasini oshirishga alohida e’tibor berilmoqda. O‘zbekistonda kiberxavfsizlikni mustahkamlash bo‘yicha davlat va xususiy sektor o‘rtasida hamkorlik aloqalari rivojlanmoqda. Biroq, ushbu sohada hali ko‘plab muammolar mavjud, jumladan, yangi tahdidlarga qarshi kurashish uchun ilg‘or texnologiyalarni joriy etish, huquqiy asoslarni mustahkamlash va aholining axborot xavfsizligi bo‘yicha xabardorligini oshirish lozim. Kelgusida ushbu vazifalarni amalga oshirish orqali mamlakat kiberxavfsizlik salohiyatini yanada oshirish mumkin.

Xulosa qilib aytganda, bugungi raqamli asrda kiberxavfsizlik har bir davlat, tashkilot va alohida shaxs uchun strategik ahamiyat kasb etmoqda. Axborot texnologiyalarining keng qo‘llanilishi nafaqat imkoniyatlarni oshirmoqda, balki turli xavf-xatarlarni ham yuzaga keltirmoqda. Kiberjinoyatlar, zararli dasturlar, ma’lumotlar o‘g‘irlanishi kabi tahdidlar butun dunyo bo‘ylab tobora kuchayib bormoqda va ular iqtisodiy, ijtimoiy hamda siyosiy barqarorlikka bevosita ta’sir ko‘rsatmoqda. Shu nuqtai nazardan, kiberxavfsizlikni ta’minlash uchun har bir foydalanuvchi, tashkilot va davlat o‘z zimmasiga mas’uliyatni olishlari zarur. Bu borada zamonaviy texnologiyalar – antivirus tizimlari, shifrlash usullari, ikki bosqichli autentifikatsiya, xavfsizlik devorlari va boshqa himoya vositalarini joriy etish bilan bir qatorda, aholining raqamli savodxonligini oshirish, xodimlarni muntazam o‘qitish va xalqaro tajribani o‘rganish kabi choralar ham muhim o‘rin

ISSN 3060-4567

tutadi. Ayniqsa, O‘zbekistonda kiberxavfsizlik sohasini mustahkamlash yo‘lida amalga oshirilayotgan islohotlar, qonunchilik bazasining takomillashuvi, mutaxassislar tayyorlash va xalqaro hamkorlikni kengaytirish bo‘yicha ko‘rilayotgan chora-tadbirlar e’tiborga molikdir. Bu esa mamlakatda axborot xavfsizligini ta’minlash, raqamli taraqqiyotga erishish hamda fuqarolarning shaxsiy ma’lumotlarini himoya qilishda muhim poydevor bo‘lib xizmat qilmoqda.

FOYDALANILGAN ADABIYOTLAR

1. O‘zbekiston Respublikasi Prezidentining 2022-yil 15-iyundagi “Kiberxavfsizlik sohasidagi davlat siyosatini takomillashtirish chora-tadbirlari to‘g‘risida”gi PQ-273-son qarori.
2. O‘zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi rasmiy sayti – https://mitc.uz
3. National Institute of Standards and Technology (NIST), “Cybersecurity Framework” – https://www.nist.gov/cyberframework
4. European Union Agency for Cybersecurity (ENISA), “Threat Landscape Report 2023” – https://www.enisa.europa.eu
5. Tanenbaum A. S., “Computer Networks”, 5th Edition, Pearson Education, 2011.
6. Stallings W., “Network Security Essentials: Applications and Standards”, 6th Edition, Pearson, 2020.
7. Kaspersky Global Research & Analysis Team (GReAT), “IT Threat Evolution Reports” – https://securelist.com
8. Symantec Corporation, “Internet Security Threat Report”, Volume 25.
9. Deloitte, “Cybersecurity Trends 2024: Risks, Resilience, and Response”.
10. Anderson R., “Security Engineering: A Guide to Building Dependable Distributed Systems”, 3rd Edition, Wiley, 2020.