VOLUME 2 | SPECIAL ISSUE 26
ISSN 2181-1784
SJIF 2022: 5.947 | ASI Factor = 1.7

O'ZBEKISTON RESPUBLIKASI JAMOAT TARTIBINI SAQLASH ORGANLARIDA KIBERXAVFSIZLIKNING O'RNI

https://doi.org/10.5281/zenodo.7336656

Rajabov Oybek Otaboyevich
O’zbekiston Respublikasi Jamoat xavfsizligi universiteti Magistratura tinglovchisi
oybek86.r@gmail.com

Annotatsiya: *Kiberxavfsizlik - kompyuterlar, uyali telefonlar yoki bulutlar deb ataladigan texnologiyalarning ishlashi uchun ma’lumotlar va hayotiy dasturlarni himoya qilishdan iborat. Umuman olganda, kiberxavfsizlik kompyuter tizimidagi muhim ma’lumotlarni (dasturiy ta’minot, kompyuter tarmoqlari, fayllar va boshqalar) tizimlar va foydalanuvchilarga zarar yetkazuvchi zararli dasturlar hujumidan himoya qilish uchun javobgardir. Hisoblash infratuzilmasi yoki axboroti uchun xavflarni minimallashtirish uchun kiberxavfsizlik ularni himoya qilishni kafolatlash uchun cheklovlar yoki protokollar kabi ko'rsatmalarni o'rnatishga imkon beradi.*

Kalit so'zlar: *Kiberxavfsizlik, texnologiya, dasturiy ta’minot, kompyuter xavfsizligi, axborot, trening, konfidensiallik.*

THE ROLE OF CYBERSECURITY IN PUBLIC ORDER PROTECTION BODIES OF THE REPUBLIC OF UZBEKISTAN

Rajabov Oybek Otaboyevich
Graduate student of Public Safety University of the Republic of Uzbekistan
oybek86.r@gmail.com

Abstract: *Cybersecurity is the protection of data and vital applications for computers, mobile phones or so-called cloud technologies. In general, cybersecurity is responsible for protecting important data in a computer system (software, computer networks, files, etc.) from malware attacks that harm systems and users. To minimize risks to computing infrastructure or information, cybersecurity allows guidelines, such as restrictions or protocols, to be established to ensure their protection.*

Keywords: *cybersecurity, technologies, software, computer security, information, training, confidentiality.*

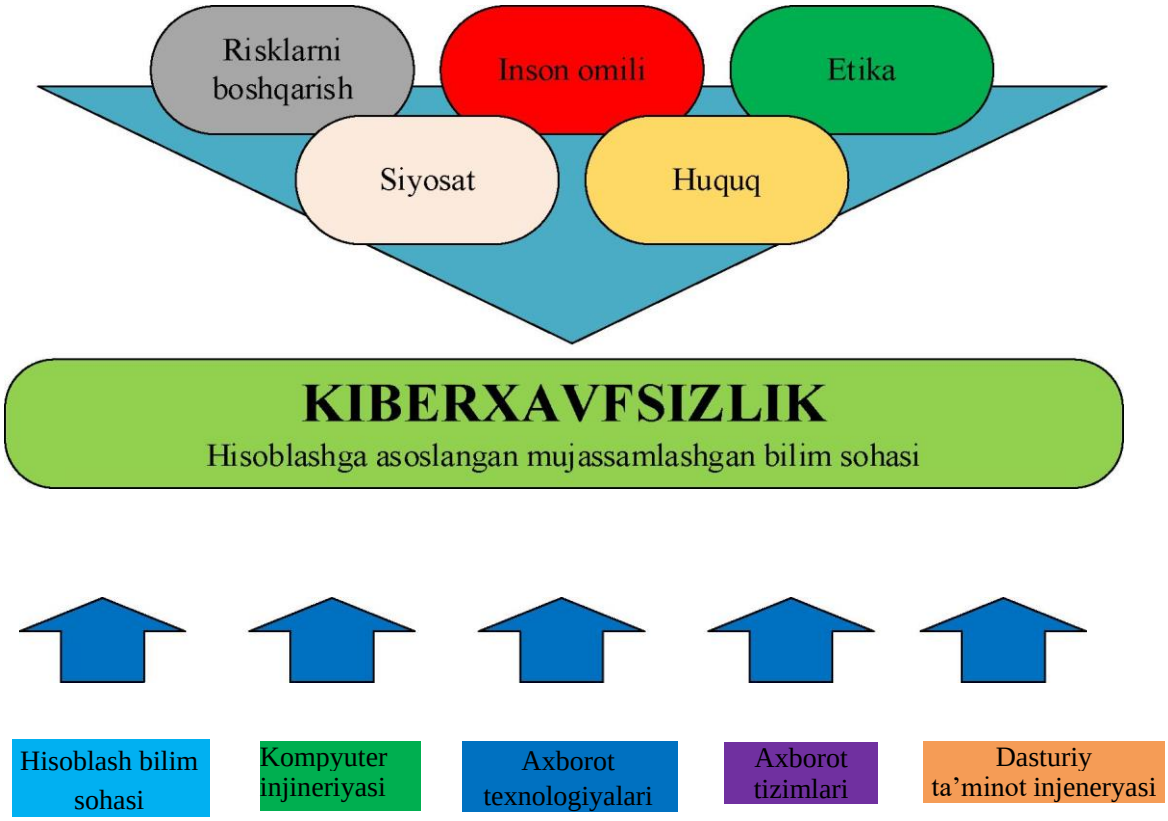
Kiberxavfsizlik bu - hisoblashlarga asoslangan bilim sohasi bo’lib, buzg’unchilar mavjud bo’lgan sharoitda amallarni to’g’ri bajarilishini kafolatlash uchun o’zida texnologiya, inson, axborot va jarayonlarni mujassamlashtiradi. U xavfsiz kompyuter tizimlarini yaratish, amalga oshirish, tahlillash va testlashni o’z ichiga oladi. Kiberxavfsizlik ta’limning mujassamlashgan bilim sohasi bo’lib, qonuniy jihatlarni, siyosatni, inson omilini, etika va risklarni boshqarishni o’z ichiga oladi.

Kiberxavfsizlik bilim sohasining zaruriyati birinchi meynfreym kompyuterlar ishlab chiqarilgandan boshlab paydo bo’la boshlagan. Bunda mazkur qurilmalarni va ularning vazifalari himoyasi uchun ko’p qatlamli xavfsizlik choralari amalga oshirilgan. Milliy xavfsizlikni ta’minlash zaruriyatini oshib borishi kompleks va texnologik murakkab ishonchli xavfsizlik choralarini paydo bo’lishiga olib keldi.

VOLUME 2 | SPECIAL ISSUE 26
ISSN 2181-1784
SJIF 2022: 5.947 | ASI Factor = 1.7

Hozirgi kunda axborot texnologiyalari sohasida faoliyat yuritayotgan har bir mutaxassisdan kiberxavfsizlikning fundamental bilimlariga ega bo’lishi talab etiladi.

1 - rasm. Kiberxavfsizlik fani sohasining tuzilishi



Konfidensiallik – axborot yoki uni eltuvchining shunday holati bo’lib, undan ruxsatsiz tanishishning yoki nusxalashning oldi olingan bo’ladi. Konfidensiallik axborotni ruxsatsiz “o’qish”dan himoyalash bilan shug’ullanadi. AOB ssenariysida Bob uchun konfidensiallik juda muhim. Ya’ni, Bob o’z balansida qancha pul borligini Tridi bilishini istamaydi. Shu sababli Bob uchun balans xususidagi ma’lumotlarning konfidensialligini ta’minlash muhim hisoblanadi.

Tizimli fikrlash - kafolatlangan amallarni ta’minlash uchun ijtimoiy va texnik cheklovlarning o’zaro ta’sirini hisobga oladigan fikrlash jarayoni. Bundan tashqari quyidagi tushunchalar ham kiberxavfsizlik sohasini chuqur o’rganishda muhim hisoblanadi.

Axborot xavfsizligi - axborotning holati bo’lib, unga binoan axborotga tasodifan yoki atayin ruxsatsiz ta’sir etishga yoki ruxsatsiz undan foydalanishga yo’l qo’yilmaydi. Yoki, axborotni texnik vositalar yordamida ishlanishida uning maxfiylik (konfidensiallik), yaxlitlik va foydalanuvchanlik kabi xarakteristikalarini (xususiyatlarini) saqlanishini ta’minlovchi axborotning himoyalanish sathi holati. Axborotni himoyalash – axborot xavfsizligini ta’minlashga yo’naltirilgan choralar kompleksi. Amalda axborotni himoyalash deganda ma’lumotlarni kiritish, saqlash, ishlash va uzatishda uning yaxlitligini, foydalanuvchanligini va agar, kerak bo’lsa, axborot va resurslarning konfidensialligini madadlash tushuniladi. Aktiv - himoyalanuvchi axborot yoki resurslar. Yoki, tashkilot uchun qimmatli barcha narsalar. Tahdid – tizim yoki tashkilotga zarar yetkazishi mumkin bo’lgan istalmagan hodisa. Yoki, tahdid - axborot xavfsizligini buzuvchi potensial yoki real mavjud xavfni tug’diruvchi sharoit va omillar majmui. Tahdid tashkilotning aktivlariga qaratilgan bo’ladi. Masalan, aktiv sifatida korxonaga tegishli biror bir saqlanuvchi hujjat bo’lsa, u holda ushbu hujjat saqlanadigan xonaga nisbatan tahdid amalga oshirilish mumkin. Zaiflik – bir yoki bir nechta

tahdidlarni amalga oshirishga imkon beruvchi tashkilot aktivi yoki boshqaruv tizimidagi kamchilik hisoblanadi. Masalan, xonada saqlanayotgan tashkilot hujjati qo’g’oz ko’rinishda bo’lganligi sababli, yonib ketishi mumkin. Boshqarish vositasi – riskni o’zgartiradigan harakatlar bo’lib, boshqarish natijasi zaiflik yoki tahdidlarni o’zgarishiga ta’sir qiladi. Bundan tashqari boshqarish vositasining o’zi turli tahdidlar foydalanishi mumkin bo’lgan zaiflikka ega bo’lishi mumkin. Masalan, tashkilotda saqlanayotgan qog’oz ko’rinishidagi axborotni yong’indan himoyalash uchun o’chirish vositalari boshqarish vositasi sifatida ko’rilishi mumkin. Bundan tashqari, yong’in bo’lganda xodimlarning xattixarakatlari va yong’inni oldini olish bo’yicha ko’rilgan chora-tadbirlar ham boshqarish vositasi hisoblanishi mumkin. Yong’inga qarshi kurashish tizimining ishlamay qolish holatiga esa boshqarish vositasidagi kamchilik sifatida qarash mumkin.

Kiberxavfsizlik va “axborot xavfsizligi” atamalaridan, tez-tez o’rnilari almashingan holatda, foydalaniladi. Ba’zilar kiberxavfsizlikni axborot xavfsizligi, axborot texnologiyalari xavfsizligi va (axborot) risklarni boshqarish tushunchalariga sinonim sifatida foydalanadilar. Ayrimlar esa, xususan, hukumat sohasidagilar kiberxavfsizlikka kompyuter jinoyatchiligi va muhim infratuzilmalar himoyasini o’z ichiga olgan milliy xavfsizlik bilan bog’liq bo’lgan texnik tushuncha sifatida qaraydilar. Turli soha xodimlari tomonidan o’z maqsadlariga moslashtirish holatlari mavjud bo’lsada, axborot xavfsizligi va kiberxavfsizlik tushunchalari orasida ba’zi muhim farqlar mavjud. Axborot xavfsizligi sohasi axborotning ifodalanishidan qat’iy nazar – qog’oz ko’rinishdagi, elektron va insonlar fikrlashida, og’zaki va vizual aloqada intelektual huquqlarini himoyalash bilan shug’ullanadi. Kiberxavfsizlik esa elektron shakldagi axborotni (barcha holatlardagi, tarmoqdan to qurilmagacha bo’lgan, o’zaro birga ishlovchi tizimlarda saqlanayotgan, uzatilayotgan va ishlanayotgan axborotni) himoyalash bilan shug’ullanadi. Bundan tashqari, hukumatlar tomonidan moliyalashtirilgan hujumlar va rivojlangan doimiy tahidlar (Advanced persistent threats, APT) ham aynan kiberxavfsizlikka tegishlidir. Qisqacha aytganda, kiberxavfsizlikni axborot xavfsizligining bir yo’nalishi deb tushunish uni to’g’ri anglashga yordam beradi.

Kuchli kiberxavfsizlik tizimiga ega bo’lishning ahamiyati, asosan, kiberhujumlarning tashkilotlarga olib keladigan ko’plab oqibatlaridan qochishdir:

• **Obro’ga putur yetkazish:** Kiberhujum mijoz, xodim yoki yetkazib beruvchi haqidagi ma’lumotlarning sizib chiqishiga olib kelishi mumkin, bu esa tashkilotdagi asosiy manfaatdor tomonlarga ishonchsizlikni keltirib chiqaradi;

• **Ma’lumotlar va jihozlarni o’g’irlash:** Ko’p hollarda kiberjinoyatchilar tashkilotlarning aloqalarini noqonuniy ravishda ushlab turadilar, shaxsiy ma’lumotlarni o’g’irlashadi va ulardan roziligisiz foydalanadilar hamda ular saqlanadigan kompyuter tizimlariga noqonuniy kirishadi;

• **Yuridik ta’sirlar:** Tashkilotlar uchinchi shaxslarning ma’lumotlarini to’g’ri himoya qilmasa, huquqiy oqibatlarga olib keladi. Shaxsiy ma’lumotlarga ta’sir ko’rsatadigan ba’zi xavfsizlik hodisalari huquqiy oqibatlarga olib kelishi va boshqa xususiy va davlat tashkilotlari tomonidan sanksiyalarga olib kelishi mumkin;

• **Axborotni yo’qotish**: Axborot kompaniyaning eng muhim aktividir. Hujjatlar barcha turdagi ma’lumotlarni o’z ichiga oladi: schyot-fakturalardan tortib mijozning shaxsiy ma’lumotlari bilan ma’lumotlar bazalarigacha. Ushbu ma’lumotlarning o’g’irlanishi yoki yo’qolishi kompaniyaning omon qolishi uchun jiddiy zarba bo’lishi mumkin.

Kiberfiribgarlik xavfini qanday kamaytirish mumkin?

Biz duch keladigan muammo murakkab xarakterga ega, tahdidlar vaqt o’tishi bilan o’zgaradi va firibgarlik sxemalarini amalga oshirishda foydalaniladigan vositalar ularga qarshi kurashish uchun ishlab chiqilgan yangi texnologiyalar va dasturiy ta’minotga moslashadi. Shu sababli, kiberfiribgarlikni aniqlash qiyin va hujumlar uzoq vaqt davomida aniqlanmasdan qolishi mumkin, bu esa tashkilotlar uchun katta firibgarlik yo’qotishlariga olib keladi. Shu sabablarga ko’ra men

profilaktikaga sarmoya kiritishni tavsiya qilaman. Kiberfiribgarlikka qarshi kurashish uchun tavsiya etilgan nazorat vositalaridan ba’zilari quyidagilardan iborat:

• **Trening:** Axborot maxfiyligi va ma’lumotlarni himoya qilish bo’yicha treningdan tashqari, firibgarlikning oldini olish va aniqlashning birinchi bosqichi tashkilotga ta’sir qilishi mumkin bo’lgan tahdidlarni (ya’ni, firibgarlik sxemalarini) bilishdir;

• **SSL sertifikatlari:** SSL (Secure Sockets Layer) sertifikatlari shifrlangan aloqa protokollari yordamida server identifikatorini autentifikatsiya qilish uchun ishlatiladi. • **Faervollar:** xavfsizlik devori va antivirusni joriy qilish tashkilotlarning kiberxavfsizligini kafolatlash uchun zarur. Faervollar - bu kompyuterdan tarmoqqa va tarmoqdan kompyuterga kirishni boshqarishga qodir kompyuter dasturlari.

•**Antimalware:** Antiviruslar, shu bilan birga, viruslar keltirib chiqaradigan infektsiyalarning oldini oladi yoki ularga qarshi kurashadi.Ular zararli dasturlar, to’lov dasturlari va Internetda tez-tez tarqaladigan viruslarning boshqa turlaridan himoya qilishni taklif qiladi;

• **Ikki faktorli autentifikatsiya (2FA):** Bu foydalanuvchi o’z shaxsini kamida ikki xil usulda tasdiqlashdan iborat xavfsizlik jarayonidir;

• **Zaxira:** Axborotni zahiralash har qanday tashkilotda vaqti-vaqti bilan amalga oshirilishi kerak bo’lgan eng muhim vazifalardan biri bo’lib, yuqori qo’shimcha qiymat taklif qiladi;

• Identifikatsiya va parolni boshqarish tizimi: Foydalanuvchining profillar, rollar va biznes qoidalari asosida mahalliy va yoki bulut ilovalariga kirishini boshqarish.

• **Xavfsiz o’chirish:** saqlangan ma’lumotlarni qaytarib bo’lmaydigan tarzda o’chirib tashlashni kafolatlash uchun fayllarni o’chirish va hatto saqlash qurilmalarini formatlash etarli emas;

• **Firibgarlik xavfini baholash:** Tashkilotga ta’sir ko’rsatishi mumkin bo’lgan firibgarlik risklari, shu jumladan kiber-firibgarlik haqida so’rov o’tkazing;

• **Mavjud boshqaruv vositalarini baholash:** Firibgarlik xavfini baholashning ikkinchi bosqichi joriy nazorat vositalari aniqlangan tahdidlarni yumshatish yoki yo’qligini aniqlashdan iborat;

Xulosa: Kiberxavfsizlik standartlari zamonaviy texnologiyalarga asoslangan biznesda katta e'tiborga ega. O'zlarining daromadlarini ko'paytirish uchun korporatsiyalar o'zlarining aksariyat operatsiyalarini Internet orqali boshqarish orqali texnologiyadan foydalanadilar. Internet tarmog'idagi operatsiyalarni keltirib chiqaradigan ko'plab xavf-xatarlar mavjud bo'lganligi sababli, bunday operatsiyalar keng qamrovli va keng ko'lamli qoidalar bilan himoyalangan bo'lishi kerak. Ushbu maqolada Kiberxavfsizlik haqida umumiy ma’lumot berib o’tilgan.

REFERENCES

1. G’aniyev S. K. ,Karimov M. M., Tashev K. A. AXBOROT XAVFSIZLIGI Toshkent 07.
2. S.S. Qosimov Axborot texnologiyalari xaqida o’quv qo’llanma Toshkent 07.
3. G’aniyev S.K.Karimov M.M. Hisoblash tizimlari va tarmoqlarida axborot xavfsizligi TDTU 03.
4. http://www.kaspersky.ru/
5. http://www.viruslist.ru/
6. http://www.citforum.ru/internet/infsecure/its2000_01.shtml/
7. http://www.osp.ru/lan/2001/04/024.htm/
8. http://www.osp.ru/lan/2001/03/024.htm/
9. www.nasa.gov/statistics/
10. www.security.uz/
11. www.cert.uz/
12. www.uzinfocom.uz/

13. Насирова, С. А., Хашимова, С. А., & Рихсиева, Г. Ш. ВЛИЯНИЕ ПОЛИТИЧЕСКОЙ СИСТЕМЫ КИТАЯ НА ФОРМИРОВАНИЕ ОБЩЕСТВЕННО-ПОЛИТИЧЕСКОЙ ТЕРМИНОЛОГИИ. *Ответственный редактор*, 162.
14. Mirzaxmedova, H. (2020). TERMS MADE FROM THE ORIGINAL IRANIAN VOCABULARY IN PERSIAN. *Philology Matters*, *2020*(1), 137-145.
15. AMANOV, K. (2015). THE MATTER OF DIVIDING AGES IN HISTORY OF TURKIC OFFICIAL METHOD. *Turkish Studies (Elektronik)*, *10*(12), 57-68.
16. Khalmurzaeva, N. T. (2020). Peculiarities of intercultural understanding in Uzbek and japanese verbal communication. *ACADEMICIA: An International Multidisciplinary Research Journal*, *10*(11), 1473-1481.
17. Abdullaevna, N. S. (2020). Lexical-semantic and cognitive specifics of political discourse (based on Si Jinping's speeches). *ACADEMICIA: An International Multidisciplinary Research Journal*, *10*(5), 1086-1092.
18. Хашимова, С. А. (2020). ОСОБЕННОСТИ ОБРАЗОВАНИЯ РЕЗУЛЬТАТИВНЫХ ГЛАГОЛОВ ПРИ ПОМОЩИ СУФФИКСАЦИИ В КИТАЙСКОМ ЯЗЫКЕ. In *Страны. Языки. Культура: сборник материалов XI-й международной научно-практической конференции/Под ред. проф. Абуевой НН Махачкала: ДГТУ. 391 с* (p. 361).
19. Omonov, Q. S., Rikhsieva, G. S., & Khalmurzaeva, N. T. (2021). THE ORIGIN OF AN OFFICIAL TURKIC STYLE AND ITS PLACE IN THE DEVELOPMENT OF A WRITTEN LITERARY LANGUAGE. *CURRENT RESEARCH JOURNAL OF PHILOLOGICAL SCIENCES (2767-3758)*, *2*(08), 45-49.
20. Hulkar, M. (2019). INTERACTIVE METHODS OF PEDAGOGICAL PROGRAMS IN TRAINING Oriental Languages. *Uzbekistan Journal of Oriental Studies*, *1*(2), 146-155.
21. OMOROV, Q. (2014). ORTA ÇAĞA AİT TÜRKÇE RESMİ YAZILARDA SÖZCÜK SEÇME MESELESİ. *Atatürk Üniversitesi Sosyal Bilimler Dergisi*, (52), 257-268.
22. Халмурзаева, Н. Т. (2020). Типология японского коммуникативно-делового этикета. *Вестник науки и образования*, (14-2 (92)), 26-30.
23. Abdullayevna, N. S. (2019). Языковая политика в Китае: идентификация общественно-политической терминологии Насирова Саодат Абдуллаевна. *КИТАЙСКАЯ ЛИНГВИСТИКА И СИНОЛОГИЯ*, *3*, 384.
24. Хашимова, С. А. (2020). ОСОБЕННОСТИ ОБРАЗОВАНИЯ РЕЗУЛЬТАТИВНЫХ ГЛАГОЛОВ ПРИ ПОМОЩИ СУФФИКСАЦИИ В КИТАЙСКОМ ЯЗЫКЕ. In *Страны. Языки. Культура: сборник материалов XI-й международной научно-практической конференции/Под ред. проф. Абуевой НН Махачкала: ДГТУ. 391 с* (p. 361).