

KIBERXAVFSIZLIKNING BUGUNGI KUNDAGI O'RNI

Nigmatov Sherzod Begzod o'g'li

*Muhammad al-Xorazmiy nomidagi Toshkent Axborot Texnologiyalar
Universiteti Samarqand filiali akademik litseyi 2-kurs talabasi*

Annotatsiya: *Mazkur maqolada zamonaviy jamiyatda kiberxavfsizlikning ahamiyati, asosiy kiber tahdidlar va axborot tizimlarini himoyalashning texnik hamda tashkiliy choralarining o'rni yoritilgan.*

Kalit so'zlar: *kiberxavfsizlik, axborot xavfsizligi, kiber tahdidlar, kiberhujumlar, zararli dasturlar (malware), fishing (phishing), tarmoq xavfsizligi, shifrlash, kiberxavfsizlik siyosati.*

THE ROLE OF CYBER SECURITY TODAY

Annotation: *This article discusses the importance of cybersecurity in today's digital environment, examines major cyber threats, and highlights the key technical and organizational measures used to protect information systems.*

Keywords: *Cybersecurity, Information Security, cyber threats, cyberattacks, malware (malware), phishing (phishing), network security, encryption, cybersecurity policy.*

РОЛЬ КИБЕРБЕЗОПАСНОСТИ СЕГОДНЯ

Аннотация: *В статье рассматривается значение кибербезопасности в современном обществе, основные виды киберугроз и меры защиты информационных систем на техническом и организационном уровнях.*

Ключевые слова: *кибербезопасность, информационная безопасность, киберугрозы, кибератаки, вредоносное ПО (вредоносное ПО), фишинг (фишинг), сетевая безопасность, шифрование, политики кибербезопасности.*

Globallashuv jarayoni va iqtisodiyotning tezkor raqamli transformatsiyasi natijasida axborot tizimlari davlat boshqaruvi, ta'lim, sog'liqni saqlash, moliya va logistika kabi sohalarning ajralmas bo'lagiga aylandi. Raqamli tizimlarning keng qo'llanilishi bilan birga ularga bo'lgan tahdidlar soni va murakkabligi ham ortib bormoqda. Natijada kiberxavfsizlik

davlat siyosati, iqtisodiy barqarorlik va jamiyat xavfsizligining asosiy omillaridan biri sifatida shakllandi.¹⁹

Axborot oqimining keskin ko'payishi, internetga ulangan qurilmalar sonining oshishi, raqamli xizmatlarning kengayishi bugun kiberxavfsizlik masalasini strategik darajaga olib chiqdi. Axborot tizimlarining ishdan chiqishi yoki ularga ruxsatsiz aralashuv sodir bo'lishi iqtisodiy jarayonlarga, davlat boshqaruviga va fuqarolar xavfsizligiga sezilarli darajada ta'sir ko'rsatishi mumkin.²⁰ Shu bilan birga, kiberxavfsizlikning ijtimoiy ahamiyati ham ortib bormoqda. Chunki kiberhujumlar ko'plab hollarda texnik vositalarga emas, balki foydalanuvchilarning noto'g'ri harakatlariga tayanadi. Xodimlarning texnik savodxonligi, foydalanuvchilarning onlayn madaniyati va tashkilotlarning xavfsizlik siyosati kiberxavfsizlik tizimining asosiy unsurlaridan biri hisoblanadi.²¹

Kiberxavfsizlikning mazmuni va asosiy vazifalari

Kiberxavfsizlik — axborot tizimlari, serverlar, kompyuter tarmoqlari, raqamli xizmatlar va foydalanuvchi ma'lumotlarini himoya qilishga qaratilgan texnik, tashkiliy va huquqiy choralar majmuidir. Hozirgi davrda axborot tizimlari iqtisodiyotning barcha tarmoqlarida asosiy resursga aylandi, shu sababli ularni himoya qilish strategik zaruriyatga aylandi.²²

Kiberxavfsizlikning asosiy vazifalari quyidagilarni o'z ichiga oladi:

1. Axborotning maxfiyligini ta'minlash,
2. Ma'lumotlarning buzilmasdan saqlanishini kafolatlash,
3. Xizmatlarning uzluksiz ishlashini ta'minlash,
4. Ruxsatsiz kirishlarning oldini olish,
5. Axborot tizimlaridagi faoliyatni monitoring qilish.

Ta'lim tizimida bu vazifalar ayniqsa muhim bo'lib, zamonaviy ta'lim muassasalari elektron jurnal, masofaviy o'qitish platformalari, onlayn test tizimlari va ma'lumotlar bazalariga bog'liq holda faoliyat yuritmoqda.²³

Zamonaviy kiberxavf turlari

Raqamli texnologiyalarning rivojlanishi bilan birga kiber tahdidlar ham murakkablashmoqda. Zamonaviy kiberhujumlar turlicha shaklga ega bo'lib, ular foydalanuvchi qurilmalariga, korxonalar tarmoqlariga yoki davlatning axborot tizimlariga zarar yetkazishi mumkin.²⁴

¹⁹ G'ulomov Sh.R, Usmanbayev D.Sh, Sayfullayev Sh.B. "Ta'lim Tizimida Kiberxavfsizlik" darslik, Toshkent-2024, 7-bet

²⁰ Ganiyev S.K, Ganiyev A.A, Xudoyqulov Z.T. "Kiberxavfsizlik asoslari" o'quv qo'llanma, Toshkent-2020, 12-bet

²¹ Skills for Care (2021) "Introduction to Cyber Security" o'quv qo'llanma 3-bet

²² Ganiyev S.K, Ganiyev A.A, Xudoyqulov Z.T. "Kiberxavfsizlik asoslari" o'quv qo'llanma, Toshkent-2020, 18-bet

²³ G'ulomov Sh.R, Usmanbayev D.Sh, Sayfullayev Sh.B. "Ta'lim Tizimida Kiberxavfsizlik" darslik, Toshkent-2024, 11-bet

²⁴ Ganiyev S.K, Ganiyev A.A, Xudoyqulov Z.T. "Kiberxavfsizlik asoslari" o'quv qo'llanma, Toshkent-2020, 12-bet

Zararli dasturlar: Malware viruslar, troyanlar, josus dasturlar, reklamaviy zararli dasturlar va kriptoshifrlar kabi shakllarda bo'lib, ular qurilma ishini izdan chiqarishi, ma'lumotlarni yashirin ravishda o'g'irlashi yoki butun tizimni bloklashi mumkin. Bugungi kunda zararli dasturlarning sun'iy intellektga asoslangan murakkab variantlari ham paydo bo'lganligi xavf darajasini yanada oshirmoqda.²⁵

Fishing hujumlari: Fishing – eng keng tarqalgan kiberhujum bo'lib, xakerlar yolg'on saytlardan, elektron pochta xabarlaridan yoki soxta havolalardan foydalanuvchi ma'lumotlarini qo'lga kiritishga harakat qiladi. Ko'plab holatlarda foydalanuvchilar ishonchli ko'ringan havolalarni bosgani sababli ma'lumotlari qo'lga tushadi.²⁶

Tarmoqqa ruxsatsiz kirish: Universitetlar, maktablar, davlat idoralari va biznes markazlarida tarmoqlarga noqonuniy kirish eng ko'p uchraydigan xavflardan biridir. Tarmoqqa kirish orqali xakerlar ma'lumotlar bazasini o'zgartirishi, foydalanuvchi hisobotlarini ko'chirib olishi yoki butun infratuzilmani ishdan chiqarishi mumkin.²⁷

Ma'lumotlarni o'g'irlash va buzish (Data Breach): Data breach holatlarida xakerlar katta hajmdagi ma'lumotlarni qo'lga kiritadi yoki ularni o'chirib yuboradi. Statistik ma'lumotlarga ko'ra, bunday hujumlar korxonalarga millionlab iqtisodiy zarar keltirishi mumkin. Ayrim holatlarda ma'lumotlar yillar davomida yashirincha o'g'irlanib kelinadi.²⁸

Davlat va jamiyat hayotida kiberxavfsizlikning o'rni

Kiberxavfsizlik davlat boshqaruvi tizimining barqaror ishlashi uchun strategik ahamiyatga ega. Raqamlashtirish jarayoni bilan bir qatorda davlat xizmatlari to'liq elektron platformalarga o'tkazilayotgani sababli davlat axborot resurslarini himoyalash masalasi ustuvor vazifaga aylandi.²⁹

Kiberxavfsizlik quyidagi tizimlarning uzluksiz ishlashini ta'minlaydi:

1. Elektron hukumat (my.gov, soliq, kadastr platformalari);
2. Moliya va bank tizimi;
3. Sog'liqni saqlashning elektron kartotipalari;
4. Ta'limning masofaviy tizimlari;
5. Transport va energetika infratuzilmalari.

Shuningdek, kiberhujumlar milliy iqtisodiyotga bevosita zarar yetkazishi mumkin. Moliyaviy ma'lumotlarning o'g'irlanishi, yirik korxonalar serverlarining ishdan chiqishi

²⁵ Skills for Care (2021) "Introduction to Cyber Security" o'quv qo'llanma 9-bet

²⁶ Federal Communications Commission (2012–2015) "Cyber Security Planning Guide" o'quv qo'llanma 12-bet

²⁷ G'ulomov Sh.R, Usmanbayev D.Sh, Sayfullayev Sh.B. "Ta'lim Tizimida Kiberxavfsizlik" darslik, Toshkent-2024, 16-bet

²⁸ Ganiyev S.K, Ganiyev A.A, Xudoyqulov Z.T. "Kiberxavfsizlik asoslari" o'quv qo'llanma, Toshkent-2020, 27-bet

²⁹ G'ulomov Sh.R, Usmanbayev D.Sh, Sayfullayev Sh.B. "Ta'lim Tizimida Kiberxavfsizlik" darslik, Toshkent-2024, 22-bet

yoki davlat sektoridagi axborot tizimlarining to'xtab qolishi iqtisodiy xavfsizlikka xavf tug'diradi.³⁰

Kiberxavfsizlikni ta'minlash strategiyalari

Texnik himoya vositalari: Axborot tizimlarini himoya qilishda shifrlash, ikki bosqichli autentifikatsiya, kirishlarni boshqarish, xavfsizlik devorlari (firewall), IDS/IPS tizimlari kabi vositalar asosiy texnik usullardir. Ular tarmoqqa ruxsatsiz kirishni aniqlash va oldini olishda yuqori samaradorlikka ega.³¹

Ma'lumotlarni tasniflash va huquqlarni boshqarish: Ma'lumotlarni maxfiylik darajasi bo'yicha toifalash, har bir foydalanuvchi uchun alohida kirish huquqlarini belgilash hamda "ko'p qatlamli mudofaa" tamoyilidan foydalanish kiberxavfsizlikning asosiy tamoyillaridan biridir.³²

Inson omili va xodimlar malakasi: Statistik ma'lumotlarga ko'ra, kiberhujumlarning 30–40 % foydalanuvchi xatolari bilan bog'liq. Xodimlarning texnik savodxonligini oshirish, muntazam treninglar o'tkazish va kiberhujumlar bo'yicha ogohlikni kuchaytirish xavfsizlikning eng muhim omillaridan biridir.³³

Ta'lim tizimida axborot xavfsizligi

Ta'lim muassasalarida axborot xavfsizligini ta'minlash uchun:

1. Tarmoq xavfsizligini kuchaytirish;
2. Talabalar va o'qituvchilarga maxsus o'quv mashg'ulotlari o'tkazish;
3. Serverlar va ma'lumotlar bazalarini muntazam yangilash;
4. Rezerv nusxalar yaratish talab etiladi³⁴

Kiberxavfsizlikning bugungi kundagi o'rni raqamli jamiyatning barqaror rivojlanishini ta'minlashda hal qiluvchi ahamiyat kasb etmoqda. Raqamli texnologiyalar hayotning barcha jabhalariga chuqur kirib borar ekan, davlat boshqaruvi, ta'lim, sog'liqni saqlash va iqtisodiyot tizimlari to'liq axborot infratuzilmasiga tayanib ishlayapti. Shuning uchun ushbu infratuzilmaning himoyalanganligi nafaqat texnik masala, balki milliy xavfsizlik va jamiyat barqarorligining strategik mezoniga aylanmoqda. Kiberhujumlarning ko'payib borishi, ularning murakkabligi va iqtisodiy zarar keltirish salohiyati kuchaygani sharoitida tashkilotlar texnik himoya vositalari bilan bir qatorda ma'lumotlar boshqaruvi, xavfsizlik siyosati va xodimlar savodxonligini takomillashtirishga majbur. Ayniqsa ta'lim

³⁰ Federal Communications Commission (2012–2015) "Cyber Security Planning Guide" o'quv qo'llanma 18-bet

³¹ Ganiyev S.K, Ganiyev A.A, Xudoyqulov Z.T. "Kiberxavfsizlik asoslari" o'quv qo'llanma, Toshkent-2020, 34-bet

³² Federal Communications Commission (2012–2015) "Cyber Security Planning Guide" o'quv qo'llanma 25-bet

³³ Skills for Care (2021) "Introduction to Cyber Security" o'quv qo'llanma 15-bet

³⁴ G'ulomov Sh.R, Usmanbayev D.Sh, Sayfullayev Sh.B. "Ta'lim Tizimida Kiberxavfsizlik" darslik, Toshkent-2024, 28-bet

tizimida tarmoq himoyasini kuchaytirish, foydalanuvchilarni muntazam o‘qitish va elektron resurslarni ishonchli boshqarish dolzarb vazifadir. Umuman olganda, zamonaviy raqamli infratuzilmaning uzluksiz ishlashi, iqtisodiy xavfsizlikning mustahkamligi va davlat xizmatlarining ishonchliligi kiberxavfsizlikning qay darajada puxta tashkil etilganiga bevosita bog‘liqdir.

Foydalanilgan adabiyotlar:

1. Ganiyev S.K, Ganiyev A.A, Xudoyqulov Z.T. “Kiberxavfsizlik asoslari” o‘quv qo‘llanma
2. G‘ulomov Sh.R, Usmanbayev D.Sh, Sayfullayev Sh.B. “Ta’lim Tizimida Kiberxavfsizlikning Muammolari Va Strategiyasi” darslik
3. Skills for Care (2021) “Introduction to Cyber Security” o‘quv qo‘llanma
4. Federal Communications Commission (2012–2015) “Cyber Security Planning Guide” o‘quv qo‘llanma