



**KIBERXAVFSIZLIK TUSHUNCHASI VA UNING TA'LIM
JARAYONIDAGI AHAMIYATI**

Dehqonova Zilolahon Mirzaevna

*Farg'ona viloyati pedagogik milliy markazi o'qituvchisi,
e-mail: zilolaziyo@umail.uz, telefon: (998) 907607575.*

Kirish

Bugungi kunda axborot texnologiyalarining jadal rivojlanishi barcha sohalar qatori ta'lim tizimini ham tubdan o'zgartirmoqda. Bu jarayon bir vaqtning o'zida turli kiberxavflarni yuzaga keltirmoqda. Shu sababli, kiberxavfsizlik nafaqat IT sohasi mutaxassislari uchun, balki ta'lim sohasidagi barcha ishtirokchilar uchun ham dolzarb tushunchaga aylanmoqda. Mazkur maqolada kiberxavfsizlik tushunchasi, uning mazmuni va ta'lim jarayonidagi ahamiyati tahlil qilinadi.

Kiberxavfsizlik tushunchasi

Kiberxavfsizlik — bu axborot texnologiyalari muhitida mavjud bo'lgan xavf-xatarlarni aniqlash, ularga qarshi choralar ko'rish va axborot resurslarini himoya qilishga qaratilgan choralar majmuasidir. Ushbu tushuncha zamonaviy hayotning barcha jabhalarini qamrab oladi. Kiberxavfsizlik shaxsiy ma'lumotlarni, moliyaviy axborotni, davlat va biznes tizimlarini himoya qilishga qaratilgan bo'lib, jamiyatda axborot madaniyatini shakllantirishning asosiy tarkibiy qismiga aylanmoqda.

Kiberxavfsizlikning ta'lim tizimidagi ahamiyati

1. Axborot madaniyatini shakllantirish

Ta'lim jarayonida kiberxavfsizlikning muhimligi ta'lim oluvchilarga axborot texnologiyalaridan xavfsiz foydalanish ko'nikmalarini singdirish orqali namoyon bo'ladi. Bu jarayonda axborot madaniyati shakllanadi, bu esa nafaqat ta'lim ishtirokchilarini, balki butun jamiyatni kiberxavf-xatarlardan himoya qilishga yordam beradi.

2. Shaxsiy ma'lumotlarni himoya qilish

Shaxsiy ma'lumotlarni himoya qilish tushunchasi

a) Shaxsiy ma'lumotlar — bu odamning shaxsiy hayoti, moliyaviy holati, sog'lig'i va boshqa shaxsiy axborotlarini ifodalovchi ma'lumotlardir. Ularni himoya qilish kiberxavfsizlikning muhim qismi hisoblanadi.

b) **Shaxsiy ma'lumotlarning xavfsizligi uchun tahdidlar**
Fishing, zararli dasturlar, ma'lumotlarni noqonuniy olish va tarqatish kabi kiberxavflar shaxsiy ma'lumotlarni xavf ostiga qo'yadi. Ayniqsa, raqamlashtirish davrida bu tahdidlar keskin o'smoqda.

Himoya tamoyillari

- a) Ma'lumotlarni yig'ish va qayta ishlashda qonuniylik va shaffoflik.
- b) Kuchli parol va shifrlash texnologiyalaridan foydalanish.
- c) Maxfiylikni saqlash va begona shaxslarga ulashmaslik.





MODERN PROBLEMS IN EDUCATION AND THEIR SCIENTIFIC SOLUTIONS

Ta'lim va xabardorlik

Shaxsiy ma'lumotlarni himoya qilishda axborot madaniyati muhim o'rin tutadi. Har bir fuqaro va tashkilotlar xabardorlikni oshirish orqali o'z ma'lumotlarini himoya qilishi lozim.

3. Onlayn o'qitishning xavfsizligini ta'minlash

So'nggi yillarda onlayn o'qitish tizimining keng tarqalishi bilan bog'liq ravishda kiberxavfsizlik muammolari yanada dolzarb bo'lib qoldi. Masofaviy ta'lim jarayonida maxfiylik va xavfsizlikni ta'minlash ta'lim tizimining samaradorligini oshirish uchun muhim ahamiyat kasb etadi.

Onlayn o'qitishning xavfsizligini ta'minlash:

Tahdidlar

tahlili:

Onlayn o'qitishda fishing hujumlari, zararli dasturlar, videoqo'ng'iroqlarni buzish va shaxsiy ma'lumotlarni o'g'irlash kabi kiberxavflar keng tarqalgan.

1. Texnik xavfsizlik choralarini ko'rish:

- Kuchli autentifikatsiya tizimlarini (ikki faktorli autentifikatsiya) joriy etish.
- Onlayn platformalarda shifrlangan aloqa (SSL/TLS) ishlatilishini ta'minlash.
- Virusga qarshi dasturlar va xavfsizlik devorlari (firewall) bilan ishlash.

3. Foydalanuvchilarni

xabardor

qilish:

Talaba va o'qituvchilarga xavfsiz internetdan foydalanish, shubhali havolalardan saqlanish va parol xavfsizligi bo'yicha bilimlar berish.

4. Maxfiylikni

ta'minlash:

Onlayn o'qitish platformalarida shaxsiy ma'lumotlarni himoya qilish bo'yicha qat'iy qoidalarni qo'llash va begona shaxslarga ulardan foydalanishga yo'l qo'ymaslik.

5. Doimiy monitoring va yangilanish:

Ta'lim platformalarining xavfsizlik tizimlarini muntazam yangilab borish va kiberxavfsizlik protokollarini doimiy ravishda nazorat qilish.

4. Kiberxavfsizlik sohasida mutaxassislar tayyorlash

Kiberxavfsizlik global muammo sifatida yangi avlod mutaxassislarini tayyorlashni talab qiladi. Ta'lim muassasalari o'quv dasturlariga kiberxavfsizlik bo'yicha maxsus kurslar kiritib, bu yo'nalishda malakali kadrlar yetishtirishga ko'maklashishi zarur.

Kiberxavfsizlikni ta'lim jarayoniga integratsiya qilish usullari

• O'quv dasturlarini boyitish

Kiberxavfsizlik bo'yicha maxsus darslar yoki qisqa kurslarni o'quv dasturlariga kiritish. Bu orqali ta'lim oluvchilarga parol xavfsizligi, phishing xurujlari, zararli dasturlardan himoya kabi masalalar o'rgatiladi.

• Amaliy mashg'ulotlar

Ta'lim oluvchilarga real kiberxavflarni bartaraf etish bo'yicha amaliy mashg'ulotlar o'tkazish. Masalan, virtual laboratoriyalarda himoya mexanizmlari bilan ishlash ko'nikmalarini shakllantirish.

• O'qituvchilar malakasini oshirish





MODERN PROBLEMS IN EDUCATION AND THEIR SCIENTIFIC SOLUTIONS

O'qituvchilarga kiberxavfsizlik bo'yicha malaka oshirish kurslarini tashkil qilish. O'qituvchi ushbu yo'nalishda bilimli bo'lsa, u ta'lim oluvchilarga to'g'ri yo'naltirish bera oladi.

Xulosa

Kiberxavfsizlik ta'lim jarayonida nafaqat texnologik muammolarni bartaraf etishga, balki ta'lim oluvchilarning umumiy axborot madaniyatini oshirishga xizmat qiladi. Bu jarayonda ta'lim muassasalarining roli katta bo'lib, ular yoshlarni zamonaviy axborot texnologiyalaridan xavfsiz foydalanishga o'rgatish bilan jamiyatda kiberxavfsizlikni ta'minlashga hissa qo'shadi. Shuningdek, davlat va xususiy sektorlar hamkorlikda ishlash orqali ta'lim tizimida kiberxavfsizlikni kuchaytirishga erishishlari lozim.

ADABIYOTLAR RO'YXATI:

1. ISO/IEC 27001:2013. **Information Security Management Systems (ISMS)**. International Organization for Standardization, 2013.
2. Whitman, M. E., & Mattord, H. J. **Principles of Information Security**. Cengage Learning, 2021.
3. Stallings, W. **Network Security Essentials: Applications and Standards**. Pearson, 2020.
4. Shmatikov, V. **Computer Security: Principles and Practice**. Addison-Wesley, 2021.
5. Anderson, R. **Security Engineering: A Guide to Building Dependable Distributed Systems**. Wiley, 2020.
6. SANS Institute. **Best Practices for Securing Online Learning Platforms**. www.sans.org, 2023.
7. Xodjaye, B. **Kiberxavfsizlik asoslari va amaliyoti**. Toshkent: O'zbekiston Milliy Universiteti nashriyoti, 2020.
8. O'zbekiston Respublikasi Prezidenti qarori. **"Raqamli O'zbekiston – 2030" strategiyasi**. Toshkent, 2020.
9. Albrechtsen, E., & Hovden, J. **The Role of Human and Organizational Factors in Cybersecurity**. Information Management & Computer Security, 2019.
10. Goh, T. T., & Sandars, J. **Increasing Cybersecurity Awareness in Online Education**. Journal of Online Learning, 2022.
11. Solove, D. J. **Understanding Privacy**. Harvard University Press, 2021.
12. O'zbekiston Respublikasi Ma'lumotlarni himoya qilish to'g'risidagi qonuni. **"Shaxsiy ma'lumotlarni himoya qilish"**. Toshkent, 2019.
13. Johnson, M. E., & Goetz, E. **Embedding Information Security into the Education Sector**. Computers & Security, 2020.
14. Yuldashev, I. **Onlayn ta'lim platformalarining xavfsizligini ta'minlash chora-tadbirlari**. "Ilmiy Innovatsiyalar Jurnali," 2021.
15. Cisco Systems. **Cybersecurity in Education: Ensuring Safe Learning Environments**. Cisco White Paper, 2023.

