

IMKONIYATI CHEKLANGAN O'QUVCHILARGA ELEKTRON XAVFSIZLIKNI O'RGATISH

Muhammadiyev Obidjon Nosirovich

*Respublika imkoniyati cheklangan shaxslar uchun
ixtisoslashtirilgan maxsus texnikumi maxsus fan o'qituvchisi*

Annotatsiya: *Ushbu maqola imkoniyati cheklangan o'quvchilarga moslangan elektron xavfsizlikni tushuntiradi. Maqsad — turli nogironlik turlariga (tayanch harakat, zaif eshituvchi) ega o'quvchilar uchun axborot va kommunikatsiya texnologiyalaridan xavfsiz foydalanishni ta'minlash bo'yicha amaliy tavsiyalar hamda texnikum va o'qituvchilar uchun chora-tadbirlarni taklif etish.*

Kalit so'zlar: *Phishing, Erişilebilir content, EDR, cloud*

KIRISH

Raqamli ta'lim vositalari va onlayn resurslar ta'lim jarayonida muhim ahamiyat kasb etadi. Imkoniyati cheklangan o'quvchilar uchun bu imkoniyatlar tenglikni ta'minlasa-da, ular uchun maxsus xavfsizlik va maxfiylik talablarini hisobga olish zarur. Ushbu maqolada xavftahlil, moslashtirilgan himoya choralari va amaliy ko'rsatmalar keltiriladi.

Elektron xavfsizlikning asosiy tamoyillari (soddalashtirilgan)

- Maxfiylik: shaxsiy ma'lumotlar faqat ruxsat etilganlar uchun ochiq bo'lsin.
- Butunlik: ma'lumotlar o'zgarmasin va ishonchli bo'lsin.
- Mavjudlik: o'quv materiallari va yordamchi texnologiyalar kerak paytda ishlaydi.

Tahdidlar va xatarlarning o'ziga xos jihatlari

- Shaxsiy ma'lumotlarning noto'g'ri tarqalishi (tug'ilgan sana, tibbiy ma'lumotlar).
- Phishing va ijtimoiy muhandislik — o'quvchi yoki ota-onani aldayish.
- Qurilmalar yo'qolishi yoki o'g'irlanishi — ekran o'qishchi, braille qurilma, planshetlar.
- Kiberzo'ravonlik va zikrlar — onlayn ta'qib, kamsitish.

Texnik va tashkilotchilik choralari (nogironlikni hisobga olgan holda)

- Kirish nazorati va autentifikatsiya:
 - Kuchli, lekin esda qolishi oson parollar; parollarni yodlash qiyin bo'lganlar uchun parol menejeri ishlatish.
 - Ikki faktorli autentifikatsiya (2FA) — SMS o'rniga brauzer/ilova tokenlari yoki apparat tokenlaridan foydalanish (ko'rish yoki jismoniy cheklovlar uchun moslashtirilgan variantlar).
- Qurilmalar va ma'lumotlarni himoya qilish:
 - Qurilmalarni shifrlash va masofaviy o'chirish funksiyasi yoqilsin.
 - Qurilmalar yo'qolsa, alternativ kirish yo'lini (ota-ona yoki vakil orqali tasdiqlash) belgilash.

- Maxfiylik va ruxsatlar:
 - O'quvchilar va ota-onalar uchun tushunarli, oddiy til bilan yozilgan maxfiylik siyosati.
 - Tibbiy va diagnostik ma'lumotlarga chek qo'yish — faqat zarur shaxslar ko'ra olishi.
- Onlayn muloqot va ijtimoiy media:
 - Shaxsiy profilni cheklash tavsiya etilsin; noqulay xabarlar bo'lsa, tezda bloklash/ozod qilish mexanizmi.
 - Yosh va imkoniyati cheklangan o'quvchilarga moslangan onlayn xulq qoidalari (visual/ovozli ko'rsatmalar).
- Erişilebilir kontent:
 - Matn uchun katta kontrast, o'lchamlash mumkin shriftlar.
 - Video materiallarda subtitles (yozuvlar) va sign language (imlo) interpretatsiyasi.
 - Rasm va diagrammalarga alt-text va audio tavsiflar.
 - Interaktiv elementlar tekshirilgan bo'lsin — klaviatura bilan boshqarish, ekran o'qishchilar bilan moslik (ARIA teglar).
- Foydalanuvchi qurilmalarida xavfsizlik dasturlari:
 - Kam resursli qurilmalar uchun yengil antivirus va yangilanishlarni avtomatik, lekin fondan bajariladigan tarzda sozlash.
 - EDR yoki murakkab vositalar o'rniga soddalashtirilgan monitoring — maktab IT bo'limi tomonidan markaziy boshqaruv.
- Zaxira va tiklash:
 - Oddiy, avtomatlashtirilgan zaxira (cloud yoki mahalliy) va tez tiklash rejasi.
 - Zaxira fayllari nutqli yoki braille formatlarda ham saqlanishi mumkin.

Pedagogik va insoniy omillar

- O'qituvchilar va xodimlarni o'qitish: imkoniyati cheklangan o'quvchilarning xavfsizligini ta'minlash bo'yicha maxsus treninglar.
- Ota-onalar bilan hamkorlik: oddiy qoidalar, xavfsiz sozlamalar bo'yicha qo'llanmalar va tez aloqa yo'li.
- Psixologik qo'llab-quvvatlash: onlayn ta'qib holatlarida tezkor yordam va xabarnoma tizimi.
- Individual ta'lim rejasi (IEP) ichida elektron xavfsizlik bandini kiritish — shaxsiy ehtiyojlarga mos choralar.

Baholash va moslashuvlar

- Baholash vositalarini moslashtirish: imtihonlarning onlayn formatida yordamchi texnologiyalar ishlatishga ruxsat.
- Autentifikatsiya va identifikatsiya jarayonlarini baholashda muqobil yo'llar (video identifikatsiya, o'qituvchi tasdiqlashi).
- Xavfsizlik choralarini sinovdan o'tkazish — imkoniyati cheklangan o'quvchilar bilan pilot testlar o'tkazish.

Huquqiy asos va standartlar

- Milliy qonunchilik va xalqaro normalarga (ma'lumotlarni himoya qilish, nogironlar huquqlari) rioya qilish.
- Ta'lim muassasalarida maxfiylik va kirish imkoniyatini ta'minlash bo'yicha siyosatlarni ishlab chiqish.

Amaliy tavsiyalar — tez yo'riq

1. Har bir o'quvchi uchun xavfsizlik va maxfiylik bo'yicha shaxsiy reja tuzilsin.
2. Maktab IT-sistemalarida kirish va ruxsatlar markazlashtirib boshqarilsin.
3. Barcha ta'lim resurslari erishilabilirlik tekshovlaridan o'tkazilsin (WCAG tamoyillari asosida).
4. Videolar uchun subtitles va sign language qo'shilsin; muqobil matn va audio tavsif taqdim etilsin.
5. O'qituvchilar va ota-onalar uchun sodda, vizual yoki audio yo'riqnomalar berilsin.
6. Favqulodda vaziyatlarda tez yordam va kontaktlar ro'yxati mavjud bo'lsin.

Xulosa

Imkoniyati cheklangan o'quvchilarga moslangan elektron xavfsizlik texnik, tashkiliy va pedagogik choralarni o'zaro uyg'unlashtirish orqali ta'minlanadi. Erişilebilirlik (accessibility) va xavfsizlik bir-birini to'ldiradi: ochiq, qulay va himoyalangan raqamli muhit yaratilsa, barcha o'quvchilar teng va xavfsiz ta'lim olish imkoniga ega bo'ladi.

FOYDALANILGAN ADABIYOTLAR:

1. World Wide Web Consortium (W3C). Web Content Accessibility Guidelines (WCAG) 2.1.
2. ISO/IEC 27001 — Information security management systems.
3. European Union. General Data Protection Regulation (GDPR).
4. UNESCO. "Guidelines for Inclusion: Ensuring Access to Education for All."
5. National Center on Accessible Educational Materials (AEM) resources.
6. NIST. "Guide to Accessible Technology" va kiberxavfsizlik bo'yicha tavsiyalar.