



TA'LIM JARAYONIDA KIBERXAVFSIZLIKNI TA'MINLASHNING USUL VA VOSITALARI TAHLILI

Yusupov Bahodir Karamatovich

PhD, professor

Axborot-kommunikatsiya texnologiyalari va aloqa harbiy instituti

Tel: +998977180560,

+998702027172, E-mail: mr_box_88@mail.ru

Rajabova Maftuna Rustamovna

Toshkent amaliy fanlar universiteti

Tel: +998998718464, E-mail: maftuna.rajabova1417@gmail.com

<https://doi.org/10.5281/zenodo.14807904>

Annotatsiya: Ushbu maqola ta'lim jarayonida kiberxavfsizlikni ta'minlashning usul va vositalari tahliliga bag'ishlangan. Bundan tashqari maqolada shaxsiy ma'lumotlarni himoyasi va onlayn ta'lim platformalarini himoya qilish oid nazariy va amaliy ma'lumotlar batafsil ko'rib chiqilgan.

Kalit so'zlar: ta'lim, kiberxavfsizlik, ta'lim texnologiyalari, usul, himoya qilish, shaxsiy ma'lumotlar, xavfsizlik choralari, elektron ta'lim, antivirus, tarmoqlararo ekran, autentifikatsiya, IDS, IPS, Google Drive, OneDrive.

Annotation: This article is devoted to the analysis of methods and means of ensuring cyber security in the educational process. In addition, theoretical and practical information on protection of personal data and protection of online educational platforms is considered in detail in the article.

Keywords: education, cyber security, educational technology, method, protection, personal data, security measures, e-learning, antivirus, firewall, authentication, IDS, IPS, Google Drive, OneDrive.

XXI-asrga kelib raqamli ta'lim jarayonlari keng miqyosda onlayn platformalar, elektron resurslar va raqamli xizmatlar bilan integratsiyalashmoqda. Bu jarayon yangi imkoniyatlar yaratish bilan birga, bir qator kibexavfsizlik muammolarini ham keltirib chiqarmoqda. Talabalar va o'qituvchilarning shaxsiy ma'lumotlarini, o'quv materiallari va ta'lim platformalarini himoya qilish muhim masalaga aylanib bormoqda. bunday xavf-xatarlardan himoyalanganlik kiberhujumlar, ma'lumotlarning o'g'irlanishi va boshqa zararli harakatlar bilan bog'liq muammolarga olib kelishi mumkin.

Kiberxavfsizlikni ta'minlash nafaqat ta'lim muassasalarining barqaror ishlashi, balki o'quvchilarning ta'lim jarayoniga oid ma'lumotlarini saqlash va ularni tashqi tahdidlardan himoyalash uchun ham zarur hisoblanadi [1].

Ta'lim jarayonlarida kiberxavfsizlikni ta'minlash tushunchasi

Ta'lim jarayonlarida kiberxavfsizlikni ta'minlash - bu o'quv muassasalarida raqamli texnologiyalar, o'quvchilarning shaxsiy ma'lumotlari, o'quv materiallari va ta'lim jarayonida ishlatiladigan barcha raqamli resurslarni kiberxavfsizlik tahdidlaridan himoya qilishga qaratilgan chora-tadbirlarning majmuasi hisoblanadi.

Kiberxavfsizlikni ta'minlash ta'lim muassasalarida o'quvchilar va xodimlarning ma'lumotlarini himoya qilish, ularga zarar yetkazilishi va ruqsatsiz kirishlardan himoyalashni ta'minlaydi. Ta'lim muassasalarida kiberxavfsizlikni ta'minlash bo'yicha amalga oshirilishi kerak bo'lgan asosiy chora-tadbirlarni quyida ko'rib chiqamiz [2, 3]:

1. **Shaxsiy ma'lumotlarni himoya qilish:** O'quvchilar, o'qituvchilar va boshqa xodimlarning shaxsiy ma'lumotlarini kriptografik himoya qilish va xavfsiz saqlash orqali ularning maxfiyligini ta'minlash zarur.

2. **Onlayn ta'lim platformalarini himoya qilish:** Masofaviy ta'lim platformalari va o'quv dasturlariga masofadan kirish (bog'lanish) xavfsizligini yaxshilash hamda buning uchun qat'iy autentifikatsiya va identifikatsiya tizimlaridan foydalanish zarur. Bu platformalar himoyalangan va foydalanuvchi ma'lumotlari yetarlicha xavfsiz saqlanishini ta'minlash kerak.

3. **Muassasa xodim va o'quvchilarini kiberxavfsizlik bo'yicha malakasini oshirish:** O'quvchilar va xodimlar kiberxavfsizlikning asosiy qoidalariga rioya qilishi uchun ularga xavfsiz parollar yaratish, phishing hujumlaridan himoyalanganlik, zararli dasturlardan saqlanish va shaxsiy qurilmalarni himoya qilish bo'yicha trening va davra suhbatlari doimiy o'tkazib borilishi kerak.



4. **Tizimga ruxsatsiz kirishlarni oldini olish:** Ta'lim muassasalarining masofaviy tizimlariga kirishni nazorat qilish uchun kuchli autentifikatsiya, ishonchli parollardan foydalanish va ikki bosqichli autentifikatsiya texnologiyalaridan foydalanish muhim ko'rsatgich hisoblanadi.

5. **Muassasa axborot tizimlarini zaxiralash nusxalash va qayta tiklash:** Ma'lumotlar yo'qotilishi yoki kiberhujumlar sodir bo'lganda, zararni minimallashtirish uchun muntazam ravishda zaxira nusxalarini yaratish va ularni xavfsiz saqlash kerak bo'ladi.

Ta'lim jarayonlarida kiberxavfsizlikni ta'minlanishi nafaqat shaxsiy ma'lumotlar xavfsizligini, balki o'quv muassasalari faoliyatining barqarorligini ham ta'minlaydi.

Ta'lim jarayonlarida kiberxavfsizlikni ta'minlash muammolari

Ta'lim jarayonlarida kiberxavfsizlikni ta'minlashda bir qancha muammolar uchraydi. Bu muammolar odatda resurslar, texnologik imkoniyatlar va bilimlarning yetarli emasligi bilan bog'liq. Ta'lim jarayonlarida kiberxavfsizlikni ta'minlash jarayonida yuzaga keladigan asosiy muammolarni quyida ko'rib chiqamiz [3, 4]:

1. **Yetarli mablag' va resurslarning yetishmasligi:** Ko'plab ta'lim muassasalari kiberxavfsizlik talablarini yaxshilash uchun zarur bo'lgan mablag' va resurslarga ega emas hisoblanadi. O'quv muassasalarida zamonaviy xavfsizlik tizimlari, antivirus dasturlari va xavfsizlik monitoringi uskunolari yetarli darajada ta'minlamagan bo'lishi mumkin.

2. **Kiberxavfsizlik bo'yicha malakali mutaxassislar yetishmasligi:** Ta'lim muassasalarida kiberxavfsizlikni ta'minlash bo'yicha yetarlicha bilim va ko'nikmalarga ega mutaxassislar yetarli darajada emas. Bu esa muassasa tizimlari va unda saqlanayotgan ma'lumotlarni himoya qilish samaradorligini pasayishiga olib keladi.

3. **Maxfiylik va shaxsiy ma'lumotlarni himoya qilishdagi qiyinchiliklar:** Talabalar va xodimlarning shaxsiy ma'lumotlarini himoya qilishda ko'plab muammolar yuzaga kelmoqda. Odatda ma'lumotlar onlayn tizimlarda saqlanadi. Agar ushbu ma'lumotlar yetarlicha himoyalansa, ular yirik kiberhujumlarni amalga oshiruvchi shaxslarga osonlik bilan qo'lga kiritilishiga olib kelishi mumkin.

4. **Kiberxavfsizlik madaniyati va xabardorlikning yetishmasligi:** Talaba, o'quvchi va xodimlar kiberxavfsizlik bilan bog'liq zaifliklardan xabardor bo'lmasligi, phishing va zararli dasturlar bilan bog'liq muammolardan xabardor bo'lmaganligi, xavfsiz parollardan foydalanmaganligi tufayli tizim himoyasini zaiflashishiga sababchi bo'lishlari mumkin.

5. **Kiberhujumlarning ortishi:** Ta'lim muassasalari himoya tizimi kiberhujumlar, masalan, DDoS (Distributed Denial of Service), zararli dasturlar, va phishing kabi hujumlarga qarshi zaif bo'lib qolishi mumkin. Kiberjinoyatchilar odatda talabalar va xodimlarning shaxsiy ma'lumotlarini yoki ta'lim muassasalarining resurslarini nishonga olishadi.

6. **Bulutli xizmatlar xavfsizligi:** Onlayn va bulutli platformalarga bo'lgan ehtiyoj ortgani sayin, bu platformalar orqali kiberxavfsizlik xavf-xatarlari ham ortib bormoqda. Bulutli xizmatlarga kirishda zaif autentifikatsiya va kriptografik himoya mexanizmlari ta'lim muassasalari axborot resurslarida katta zarar yetkazishi mumkin.

7. **Himoya vositalarini uzluksiz yangilanish va doimiy fizik himoyani tashkil etishning murakkabligi:** Ta'lim muassasalarida axborot xavfsizligi vositalarini muntazam yangilash va xavfsizlik tizimini doimiy nazorat qilish hamda fizik himoyalash ko'p vaqt va mablag' talab qiladi, shunga qaramay barcha muassasalar buni to'liq ta'minlay olmaydi [4].

Ushbu muammolarni hal qilishda o'quv muassasalarida kiberxavfsizlikni ta'minlashning asosiy qoidalariga rioya qilish, xodim va o'quvchilarga treninglar o'tkazish va kiberxavfsizlik infrastrukturasi uchun mablag' ajratishni yo'lga qo'yish zarur masalalardan biri hisoblanadi.

Ta'lim jarayonlarida kiberxavfsizlikni ta'minlash muammolari tahlili
1- jadvalda keltirilgan.

1-jadval

Ta'lim jarayonlarida kiberxavfsizlikni ta'minlash muammolari tahlili



Muammolar	Izoh	Ta'siri	Hal qilish usullari
Mablag' va resurslar yetishmasligi	Kiberxavfsizlik choralarga mablag' yetarli ajratilmasligi	Xavfsizlik darajasi past, tarmoq hujumlarga nisbatan zaiflikni yuzaga kelishi	Moliyaviy ko'mak, grant va hukumat dasturlaridan foydalanish
Mutaxassislar yetishmasligi	Kiberxavfsizlik bo'yicha tajribali kadrlar yo'qligi	Xavfsizlikni ta'minlash bilan bog'liq samaradorlikni pasayishi	Malakali mutaxassislarni jalb qilish yoki mavjud xodimlarni o'qitish
Shaxsiy Ma'lumotlarni himoya qilishdagi qiyinchiliklar	Talabalar va xodimlarning ma'lumotlarini xavfsiz saqlash murakkab yondashuvni talab qiladi	Ma'lumotlarning ruxsatsiz chiqib ketishi, maxfiylikning buzilishi	Kriptografik himoyalash va tizimga ruxsat etilmagan kirish huquqini cheklash, maxfiylik siyosatini joriy etish
Kiberxavfsizlik madaniyatining yetarli emasligi	Foydalanuvchilarning kiberxavfsizlik talablaridan xabardor emasligi	Kiberhujumlar xavfi ortishi	kiberxavfsizlik bo'yicha muntazam trening va seminarlar o'tkazish
Kiberhujumlarning ortishi	DDoS, zararli dasturlar va phishing hujumlarining ko'payishi	O'quv jarayoniga to'sqinlik qilishi, ma'lumotlarning ruxsatsiz chiqib ketishi yoki shikastlanishi	Tarmoqlararo ekran, antiviruslar dasturlari va boshqa himoya vositalarini kuchaytirish
Bulutli xizmatlar xavfsizligi	Bulutli platformalarda ma'lumotlarni boshqarish va xavfsiz saqlash qiyinligi	Bulutli xizmatlardan ruxsatsiz foydalanish, ma'lumotlar maxfiyligini xavf ostida qolishi	Kriptografik himoyalash va kuchli autentifikatsiya hamda tizimdan ruxsat etilmagan foydalanishni cheklash
Himoya vositalarini yangilanish va nazoratning murakkabligi	Xavfsizlik tizimlarini muntazam yangilab turish zaruriyati	Yaroqsiz dasturlar yoki texnologiyalar tufayli kiberhujumlarga zaifliklarni ortishi	Muntazam ravishda himoya vositalarini yangilanshni joriy qilish va xavfsizlik monitoring qiluvchi tizimlarni o'rnatish

1.1- jadvalda keltirilgan tahlil natijalari himoya vositalari bilan bog'liq muammolarni tizimli ravishda ko'rib chiqishga yordam beradi. Bu esa kiberhujum va ularning oqibatlarini va ularga yechim topish uchun zarur choralarini belgilab olishga zamin yaratadi [4].

Ta'lim jarayonlarida kiberxavfsizlikni ta'minlash usullari

Ta'lim jarayonlarida kiberxavfsizlikni taminlash uchun bir qancha samarali usullar mavjud [5, 6]:

1. Shaxsiy ma'lumotlarni himoya qilish



O'zbekistonda joylashgan ba'zi universitetlar talabalari va o'qituvchilarining shaxsiy ma'lumotlarini, baholarini, moliyaviy ma'lumotlarini himoya qilish uchun o'z tizimlarida kriptografik himoya vositalari va ta'lim tizimi platformalariga kirish huquqini cheklash mexanizmlari joriy qilinadi. Masalan, faqat shaxsiy parol va login orqali kiritilganda, talabani shaxsiy kabinetiga boshqa biror g'arazli shaxs tomonidan tizimga kirish mumkin bo'ladi [7].

2. Foydalanuvchilar uchun kiberxavfsizlik treninglarini tashkil etish va xabardorlikni oshirish

Ko'plab maktab va universitetlar o'quvchilarga kiberxavfsizlikka oid seminar va treninglar o'tkazib kelmoqda. Bu treninglarda ularga phishing hurujlarini amalga oshirish bo'yicha dastlabki ma'lumotlar, zararli havolalardan saqlanish, shaxsiy qurilmalarini himoya qilish kabi nazariy va amaliy ko'nikmalar o'rgatiladi. Masalan, ular o'zlarining ijtimoiy tarmoqlarida noma'lum havolalarni ochmaslik va mustahkam parollar ishlatish muhimligini bilib olishadi.

3. Ikki bosqichli autentifikatsiya (2FA)

AQSHda ba'zi ta'lim muassasalari o'qituvchilar va talabalar uchun ta'lim platformalarida ikki bosqichli autentifikatsiya tizimini joriy etgan. Masalan, universitetning elektron pochta tizimiga kirish uchun parol bilan birga foydalanuvchining telefoniga SMS orqali yuboriladigan tasdiq kodi kerak bo'ladi. Bu qo'shimcha bosqich foydalanuvchilarning akkauntiga ruxsat etilmagan kirishlardan himoyani ta'minlash imkonini beradi.

4. Antivirus va tarmoqlararo ekran (firewall)

Maktab yoki universitet kompyuter tarmoqlarida antivirus dasturlari o'rnatilgan bo'lib, ular zararli dasturlarni aniqlab, bloklash yoki o'chiqishni amalga oshiradi. Tarmoqlararo ekran esa ichki tarmoq va tashqi tarmoq o'rtasida xavfsizlikni ta'minlashda o'rtadagi filtr bo'lib xizmat qiladi, bu orqali faqat ruxsat etilgan trafikka ruxsat beriladi.

5. Ma'lumotlarni muntazam zaxirali nusxalash

Maktablar yoki universitetlar o'zlarining o'quv dasturlarini va o'quvchilarning baholarini bulutda yoki mahalliy serverda muntazam ravishda zaxirali nusxalab borishlari kerak. Masalan, "Google Drive" yoki "OneDrive" kabi bulut xizmatlaridan foydalanib, barcha muhim ma'lumotlar yo'qotilgan taqdirda ham ularni tezda tiklash mumkin bo'ladi.

6. Kirish huquqlarini nazorat qilish va boshqarish

Ba'zi universitetlar faqat ruxsat etilgan shaxslarga kirish huquqlarini ta'minlash uchun foydalanuvchilarga ularning roliga mos tizim resurslaridan foydalanishga ruxsat berishadi. Masalan, talaba faqat o'z baholarini ko'rishi mumkin, lekin boshqa talabalar yoki xodimlarning ma'lumotlarini ko'rish imkoniyatiga ega bo'lmaydi.

7. Kiberhujumlarni aniqlash va ularni oldini olish tizimlari (IDS/IPS)

Ba'zi yirik universitetlarda ta'lim tizimini boshqarish platformalarida ruxsatsiz kirishni aniqlash (IDS) va ruxsatsiz kirishni oldini olish (IPS) tizimlari qo'llanadi. Bu tizimlar kiberhujumlar yoki shubhali harakatlarni avtomatik aniqlaydi va ularni bloklash imkonini taqdim etadi. Misol uchun, universitet tarmog'ida noodatiy yoki zararli faoliyat sezilsa, IPS tizimi avtomatik ravishda bu faoliyatni bloklaydi [8].

Xulosa qilib aytadigan bo'lsak, yuqorida ko'rib chiqilgan himoya usullari va vositalari ta'lim jarayonida kiberxavfsizlikni ta'minlashga yordam beradi va o'qituvchilar, o'quvchilar va xodimlarning shaxsiy hamda konfidensial ma'lumotlarini himoyalash imkonini yanada yaxshilash imkonini beradi.

Foydalanilgan adabiyotlar ro'yxati

1. Majeed, A.; Alnajim, A.M.; Waseem, A.; Khaliq, A.; Naveed, A.; Habib, S.; Islam, M.; Khan, S. Deep Learning-Based Symptomizing Cyber Threats Using Adaptive 5G Shared Slice Security Approaches. *Future Internet* 2023, 15, 193.
2. Alnajim, A.M.; Habib, S.; Islam, M.; Albelaihi, R.; Alabdulatif, A. Mitigating the Risks of Malware Attacks with Deep Learning Techniques. *Electronics* 2023, 12, 3166.
3. Sharma, R. (2021). Data Protection and Privacy in the Education Sector. *Cybersecurity Journal*, 12(3), 45-60.



4. Morrison, C. (2022). Educational Technology and Cybersecurity. Routledge.
5. National Institute of Standards and Technology (NIST). (2018). Cybersecurity Framework. Available at: <https://www.nist.gov>
6. Brown, M. (2021). Two-Factor Authentication and Its Role in Cybersecurity for Schools. Journal of Digital Security, 9(2), 13-28.
7. International Society for Technology in Education (ISTE). (2019). Cybersecurity Awareness and Education in Schools.
8. Jones, P. (2020). The Role of Antivirus and Firewalls in Educational Cybersecurity. Journal of Information Security, 14(1), 98-115..