



KASBIY FAOLIYATDA AXBOROT TEXNOLOGIYALARIDAN FOYDALANISH VA AXBOROT XAVFSIZLIGINI TA'MINLASH

Uzun tuman 3-son texnikumi

Maxsus fan o'qituvchisi

Tojiddinova Gulnora To'lanbek qizi

gulnoratojiddinova07@gmail.com

Annotatsiya: Ushbu maqola zamonaviy kasbiy faoliyatda axborot texnologiyalaridan foydalanishning ahamiyati va shu jarayonda axborot xavfsizligini ta'minlash masalalarini o'rganishga bag'ishlangan. Maqolada axborot texnologiyalari kasbiy faoliyatni samarali qilishi, shuningdek, axborot xavfsizligi tahdidlarini kamaytirish yo'llari tahlil qilingan. O'qituvchi nuqtayi nazaridan o'quvchilarga axborot xavfsizligi ko'nikmalarini shakllantirish bo'yicha amaliy tavsiyalar berilgan.

Kalit so'zlar: Axborot texnologiyalari, axborot xavfsizligi, kasbiy faoliyat, pedagogik yondashuv, raqamli kompetensiya, kiberxavfsizlik, ta'lim jarayoni, xavfsizlik strategiyalari.

Annotation: This article is devoted to the study of the importance of using information technologies in modern professional activities, as well as to the issues of ensuring information security in this process. The article analyzes how information technologies enhance the efficiency of professional activities and examines ways to reduce information security threats. From the teacher's perspective, practical recommendations are provided for developing students' information security skills.

Key words: Information technologies, information security, professional activity, pedagogical approach, digital competence, cybersecurity, educational process, security strategies.



Аннотация: Данная статья посвящена изучению значения использования информационных технологий в современной профессиональной деятельности, а также вопросам обеспечения информационной безопасности в этом процессе. В статье анализируется, как информационные технологии повышают эффективность профессиональной деятельности, а также рассматриваются пути снижения угроз информационной безопасности. С точки зрения преподавателя представлены практические рекомендации по формированию у обучающихся навыков информационной безопасности.

Ключевые слова: Информационные технологии, информационная безопасность, профессиональная деятельность, педагогический подход, цифровая компетенция, кибербезопасность, образовательный процесс, стратегии безопасности.

KIRISH

Zamonaviy kasbiy faoliyat sohalari axborot texnologiyalarini bevosita o'z faoliyatiga integratsiya qilgan. Texnologiyalar yordamida ish jarayonlari tezkor, samarali va sifatli amalga oshiriladi. Misol uchun, moliya va bank sohasida avtomatlashtirilgan hisob-kitob tizimlari ish jarayonlarini sezilarli darajada soddalashtiradi, sog'liqni saqlash tizimida elektron kartoteka va masofaviy diagnostika xizmatlari sifatni oshiradi, ta'limda esa elektron darsliklar va interaktiv mashg'ulotlar o'quv jarayonini boyitadi [1].

Shu bilan birga, AT dan foydalangan holda axborot xavfsizligi masalalari dolzarb bo'lib qolmoqda. Axborot xavfsizligi — bu axborot tizimlari va ularda saqlanayotgan ma'lumotlarni zararli ta'sirlardan, kiberhujumlardan va noto'g'ri foydalanishdan himoya qilish jarayoni [2]. Global tadqiqotlar shuni ko'rsatadiki, dunyoda kiberhujumlar soni yildan-yilga oshib bormoqda va bu kasbiy faoliyatdagi jarayonlarga salbiy ta'sir ko'rsatadi [3].

O'qituvchi nuqtayi nazaridan, kasbiy faoliyatda AT va axborot xavfsizligini birlashtirib o'qitish — o'quvchilarda nafaqat texnik bilimlarni, balki xavfsizlik madaniyatini shakllantirishga xizmat qiladi. Bugungi kunda ta'lim tizimida raqamli



kompetensiyalarni rivojlantirish, xavfsizlik protokollarini o'rgatish va real misollar orqali tahdidlarni tushuntirish pedagogik jarayonning ajralmas qismiga aylanmoqda [4].

Bunda ushbu muammo mavjud: Ko'plab mutaxassislar AT dan foydalanish jarayonida xavfsizlik qoidalarini yetarlicha bilmaydi yoki amalda qo'llay olmaydi. Bu esa, ma'lumotlarning yo'qolishi, shaxsiy va kasbiy ma'lumotlarning oshkor bo'lishiga olib keladi.

Yuqorida keltirilgan muammoga quyidagicha yechimlar berish mumkin:

- o'quv jarayoniga axborot xavfsizligi mavzusini integratsiyalash;
- o'quvchilarni kiberxavfsizlik bo'yicha amaliy mashg'ulotlar bilan shug'ullantirish;
- kasbiy faoliyatda xavfsizlik protokollarini doimiy qo'llash. Shunday qilib, mazkur maqola kasbiy faoliyatda AT'dan foydalanish va xavfsizlikni ta'minlash masalalarini tizimli tahlil qiladi va pedagogik yondashuvni asosiy vosita sifatida ko'rsatadi.

ASOSIY QISM

1. Kasbiy faoliyatda axborot texnologiyalarining ro'li. AT kasbiy faoliyatni quyidagi yo'nalishlarda transformatsiya qilmoqda:

- **Ma'lumotlarni tezkor qayta ishlash va saqlash:** zamonaviy dasturiy vositalar ma'lumotlar bazasini boshqarish, katta hajmdagi ma'lumotlarni tahlil qilish va saqlash imkonini beradi [5].

- **Kommunikatsiya va hamkorlik:** onlayn platformalar, elektron pochta, videokonferensiyalar mutaxassislarning o'zaro hamkorligini sezilarli darajada oshiradi [6].

- **Qaror qabul qilishni qo'llab-quvvatlash:** analitik vositalar va ma'lumotlarni vizualizatsiya qilish texnologiyalari rahbarlar va mutaxassislar uchun tezkor va ishonchli qaror qabul qilish imkonini yaratadi [7].



- **Kasbiy kompetensiyalarni rivojlantirish:** o'quvchilarda raqamli kompetensiyalarni rivojlantirish, dasturlash, ma'lumotlar bilan ishlash, axborot xavfsizligini tushunish imkonini beradi [8].

O'qituvchi nuqtayi nazaridan, AT dars jarayonida interaktiv taqdimotlar, simulyatsiyalar, masofaviy laboratoriya mashg'ulotlari orqali o'quvchilarning amaliy ko'nikmalarini oshirish mumkin. Bu pedagogik jarayonda nafaqat texnik bilim, balki xavfsizlik madaniyatini ham shakllantiradi.

2. Axborot xavfsizligi tahdidlari va xavf turlari. Kasbiy faoliyatda AT'dan foydalanish bilan birga quyidagi tahdidlar mavjud:

- **Kiberhujumlar va zararli dasturlar:** viruslar, trojanlar, ransomware dasturlari tizimlarga zarar yetkazadi va ma'lumotlarni yo'qotadi [9].

- **Ma'lumotlarning oshkor bo'lishi:** shaxsiy va kasbiy ma'lumotlar noto'g'ri qo'llanilganda maxfiylik buziladi [10].

- **Foydalanuvchi xatolari:** zaif parollar, xavfsizlik protokollariga amal qilmaslik va firibgarlik (phishing) xavfini oshiradi [11].

- **Tashkiliy xatoliklar:** kompaniya siyosatining yetarlicha ishlab chiqilmaganligi xavfsizlikni zaiflashtiradi.

3. Axborot xavfsizligini ta'minlash strategiyalari. Kasbiy faoliyatda axborot xavfsizligini ta'minlash uchun samarali strategiya **texnik, tashkiliy va pedagogik choralarni uyg'un qo'llashga** asoslangan bo'lishi kerak. Har bir chora-tadbirning o'ziga xos ro'li va samaradorligi mavjud.

A. Texnik chora-tadbirlar.

Texnik chora-tadbirlar — axborot tizimlarini, ma'lumotlarni va kommunikatsiyalarni zararli ta'sirlardan himoya qilishga qaratilgan dasturiy va apparat vositalaridir. Ushbu chora-tadbirlar kasbiy faoliyatda eng asosiy va tezkor natija beruvchi vosita hisoblanadi.

1. Antivirus va firewall dasturlarini joriy etish:



1) **Antivirus dasturlari** zararli dasturlarni (viruslar, trojanlar, ransomware) aniqlash va yo'q qilish imkonini beradi. Bu o'qituvchilar va o'quvchilar tomonidan ishlatiladigan kompyuter va serverlarni himoya qilishda asosiy chora hisoblanadi.

2) **Firewall** — tarmoq xavfsizligini ta'minlash vositasi bo'lib, ruxsatsiz kirishlarni bloklaydi va tarmoqdagi trafikni nazorat qiladi. Masalan, kompaniya yoki ta'lim muassasasi lokal tarmog'ida firewall yordamida tashqi tahdidlardan himoyalaniishi mumkin [12].

2. Ma'lumotlarni shifrlash va zaxira nusxasini yaratish:

1) **Shifrlash** — ma'lumotlarni kodlash orqali ularni ruxsatsiz shaxslar tomonidan o'qilmasligini ta'minlaydi. Bu elektron pochta, bulutli saqlash va masofaviy ish platformalarida muhimdir.

2) **Zaxira nusxasi (backup)** — ma'lumotlar yo'qolishi yoki buzilishiga qarshi chora. Masalan, muassasa serverida kundalik va haftalik backup yaratish orqali kiberhujumlar, texnik nosozlik yoki inson xatolaridan kelib chiqadigan xavflardan saqlanish mumkin.

3. Tizimga kirish ruxsatlarini boshqarish:

Har bir foydalanuvchi faqat o'z ish vazifalari uchun zarur bo'lgan tizim resurslariga kirishi kerak. Bu prinsip “minimal huquq” (least privilege) deb ataladi. Masalan, o'quvchilar faqat o'quv resurslariga kirishi mumkin, administrator esa barcha tizimni boshqaradi. Bu xatolik va ma'lumotlar buzilishi xavfini sezilarli darajada kamaytiradi. Texnik choralar yuqori samaradorlikni beradi (jadvaldagi 85–90%), ammo ular inson faktorini qamrab olmaydi. Shu sababli texnik choralar pedagogik va tashkiliy choralarsiz yetarli emas.

B. Tashkiliy chora-tadbirlar.

Tashkiliy chora-tadbirlar — axborot xavfsizligini ta'minlashda **muassasa siyosati, me'yoriy hujjatlar va nazorat tizimi** orqali amalga oshiriladi.



1. Axborot xavfsizligi siyosatini ishlab chiqish. Har bir tashkilot yoki ta'lim muassasasi xavfsizlik strategiyasini yozma shaklda ishlab chiqishi lozim. Bu siyosatda:

- foydalanuvchilarning majburiyatlari;
- ma'lumotlarni saqlash va uzatish qoidalari;
- tahdid va xatoliklarni aniqlash tartibi;
- javobgarlik mexanizmlari kiritiladi.

Masalan, universitetda elektron ma'lumotlar bazasiga kirish qoidalari va shaxsiy ma'lumotlarni himoya qilish siyosati mavjud bo'lishi shart.

2. O'qituvchilar va o'quvchilar uchun xavfsizlik qoidalari bo'yicha treninglar o'tkazish. O'quv va ish jarayonida foydalanuvchilarni xavfsizlik qoidalariga o'rgatish muhimdir. Treninglar real hayot misollariga asoslangan bo'lishi kerak: phishing xatolari, zaif parollar, zararli dasturlarni aniqlash va ulardan saqlanish. Misol uchun, har chorakda o'quvchilar va o'qituvchilar uchun kiberxavfsizlik bo'yicha interaktiv seminarlar va testlar o'tkaziladi [13].

3. Ma'lumotlar oqimini nazorat qilish. Ma'lumotlar kirishi, uzatilishi va saqlanishi doimiy ravishda monitoring qilinishi kerak. Masalan, o'quvchilar tizimga kirish paytida ularning ish faoliyati log fayllarida saqlanadi va shubhali harakatlar aniqlanadi. Bu tahdidlarni erta bosqichda aniqlash va zararni kamaytirishga yordam beradi.

Tashkiliy chora-tadbirlar texnik choralarni mustahkamlash bilan birga foydalanuvchi xatolarini kamaytiradi. Ular xavfsizlikni tizimli ravishda boshqarish imkonini beradi va inson faktoriga bog'liq tahdidlarni kamaytiradi.

C. Pedagogik chora-tadbirlar.

Pedagogik chora-tadbirlar — *o'qituvchi va o'quvchilar o'rtasidagi bilim va ko'nikmalarni shakllantirish* orqali xavfsizlikni ta'minlashga qaratilgan.



1. O'quvchilarni kiberxavfsizlik va xavfsiz axborot tizimlari bo'yicha o'qitish.

O'quv dasturiga kiberxavfsizlik bo'yicha alohida fan kiritish. O'quvchilar shaxsiy va kasbiy ma'lumotlarni himoya qilish, parollarni xavfsiz boshqarish, xavfli havolalardan saqlanish kabi ko'nikmalarni egallaydi.

2. Amaliy mashg'ulotlar va testlar orqali bilimlarni mustahkamlash. Nazariy bilim yetarli emas, amaliy mashg'ulotlar orqali o'quvchilar xavf va tahdidlarni aniqlashni o'rganadi. Masalan, simulyatsiya orqali phishing hujumini aniqlash yoki xavfsiz parol yaratish bo'yicha topshiriqlar beriladi.

3. Raqamli madaniyat va etikani shakllantirish. O'quvchilar raqamli etikani va axborot madaniyatini o'rganishi zarur. Bu ularni nafaqat kasbiy faoliyatda, balki shaxsiy hayotida ham xavfsiz ishlashga o'rgatadi. Misol uchun, o'quvchilar onlayn platformalarda xatti-harakatlarni nazorat qilish, ma'lumotlarni o'zgartirish va tarqatishdan oldin etik qoidalarini hisobga olishni o'rganadi.

Pedagogik chora-tadbirlar, texnik va tashkiliy choralarning samaradorligini oshiradi. Foydalanuvchilarning bilim darajasi yuqori bo'lsa, kiberxavfsizlik tahdidlari sezilarli darajada kamayadi. Shu bilan birga, u kasbiy faoliyatga tayyorgarlik va raqamli kompetensiyalarni rivojlantirishga xizmat qiladi.

O'qituvchi sifatida, AT darslarida xavfsizlik qoidalarini amaliy mashg'ulotlarda qo'llash va interaktiv testlar orqali o'quvchilarni o'rgatish samarali usul hisoblanadi.

4. O'qituvchi va o'quvchining ro'li.

O'qituvchi:

- AT vositalarini samarali qo'llash;
- axborot xavfsizligi choralarini o'rgatish;
- o'quvchilarni real misollar va vaziyatlar orqali o'rgatish;

O'quvchi:

- xavfsizlik qoidalariga rioya qilish;
- shaxsiy va kasbiy ma'lumotlarni himoya qilish;



- masofaviy va raqamli platformalarda xavfsizlikni ta'minlash [14].

TAHLIL VA NATIJALAR

Maqola doirasida quyidagi kutiladigan natijalar belgilanishi mumkin:

- kasbiy faoliyatda AT samaradorligi oshadi;
- axborot xavfsizligi bo'yicha bilim va ko'nikmalar shakllanadi;
- kiberxavfsizlik tahdidlariga qarshi chora-tadbirlar qo'llanadi.

1-jadval

Axborot xavfsizligi choralarining samaradorligi

T/r	Chora turi	Samaradorli	Sharh
1.	Antivirus	85	Zararlanish xavfini kamaytiradi
2.	Parol siyosati	70	Foydalanuvchi xavfsizligini oshiradi
3.	Shifrlash	90	Ma'lumotlarni himoya qiladi
4.	Ta'lim va trening	75	Kiberxavfsizlik madaniyatini oshiradi

Jadvaldagi ma'lumotlar kasbiy faoliyatda axborot xavfsizligini ta'minlashning samaradorligini turli chora-tadbirlar nuqtai nazaridan ko'rsatadi:

1. Antivirus dasturlari (85%). Antivirus va zararli dasturlarga qarshi vositalar tizimlarni himoya qilishning eng asosiy texnik chorasi hisoblanadi. 85% samaradorlik ko'rsatkichidan ko'rinib turibdiki, antivirus dasturlarining joriy etilishi tizimdagi zararli fayllarni aniqlash va ularni yo'q qilish imkonini beradi. Shu bilan birga, ular kiberhujumlarga qarshi birinchi chiziq bo'lib xizmat qiladi. Lekin antivirus texnik vosita sifatida yolg'iz yetarli emas, chunki foydalanuvchi xatolari yoki zaif parollar orqali tizimga kirish xavfi qoladi.

2. Parol siyosati (70%). Parol siyosati xavfsizlikning asosiy inson faktoriga bog'liq qismi bo'lib, foydalanuvchilarning kirish ma'lumotlarini himoya qiladi. 70% samaradorlik raqami shuni ko'rsatadiki, kuchli va murakkab parollar foydalanuvchi



ma'lumotlarini himoya qilsa-da, odatda foydalanuvchilar oddiy parollarni tanlashi xavfsizlikni kamaytiradi. Shu sababli parol siyosati boshqa texnik va pedagogik choralar bilan birlashtirilganda maksimal samaradorlikka erishadi.

3. Shifrlash (90%). Ma'lumotlarni shifrlash eng yuqori samaradorlik ko'rsatkichiga ega (90%). Bu texnik chora ma'lumotlarning himoyasini kafolatlaydi, ularni maxfiylikni saqlaydi va ruxsatsiz kirishdan himoya qiladi. Ayniqsa, elektron pochta, bulutli saqlash va masofaviy ish jarayonlarida shifrlash muhim ahamiyat kasb etadi. Shifrlashning samaradorligi yuqori bo'lsa-da, u ham foydalanuvchi xatolaridan mustasno emas; masalan, parolni noto'g'ri boshqarish yoki shifrlash kalitlarini oshkor qilish xavfini kamaytiradi.

4. Ta'lim va trening (75%). Pedagogik choralar — o'quvchilar va o'qituvchilarni kiberxavfsizlik bo'yicha o'qitish va treninglar o'tkazish — tizim xavfsizligini oshirishda muhim ro'l o'ynaydi. 75% samaradorlik, texnik choralar bilan birlashtirilganda, foydalanuvchilarni xavf va tahdidlarni aniqlash, ulardan saqlanish hamda xavfsizlik protokollariga amal qilishga o'rgatadi. Ta'lim orqali shakllantirilgan xavfsizlik madaniyati uzoq muddatda samaradorlikni oshiradi va kiberxavfsizlik tahdidlarini sezilarli darajada kamaytiradi.

Jadvaldan ko'rinib turibdiki, texnik chora-tadbirlar (antivirus va shifrlash) yuqori samaradorlikni beradi, ammo inson faktori (parol siyosati va trening) bilan birlashtirilmasa, tizim xavfsizligi to'liq kafolatlanmaydi. Shu sababli kasbiy faoliyatda axborot xavfsizligini ta'minlash strategiyasi **texnik, tashkiliy va pedagogik choralarni uyg'un qo'llash**ga asoslangan bo'lishi lozim.

Bundan kelib chiqadiki, **o'qituvchining ro'li** o'quvchilarda xavfsizlik madaniyatini shakllantirishda, amaliy mashg'ulotlar va real hayot misollarini qo'llashda muhim ahamiyatga ega. Bu esa nafaqat kasbiy faoliyatda xavfsizlikni oshiradi, balki AT samaradorligini maksimal darajaga chiqaradi.

XULOSA



Texnik, tashkiliy va pedagogik chora-tadbirlarni birlashtirish kasbiy faoliyatda axborot xavfsizligini maksimal darajada ta'minlaydi. Har bir chora o'zaro bog'liq bo'lib, umumiy xavfsizlik tizimini yaratadi: texnik choralar tizimni himoya qiladi, tashkiliy choralar foydalanuvchi va jarayonlarni boshqaradi, pedagogik choralar esa inson faktorini kuchaytiradi. Shu sababli, o'qituvchi va mutaxassislarning bilim va ko'nikmalarini rivojlantirish xavfsizlik strategiyasining ajralmas qismi hisoblanadi.

Kasbiy faoliyatda axborot texnologiyalaridan foydalanish samaradorlikni oshiradi, lekin axborot xavfsizligi tahdidlarini e'tiborsiz qoldirish mumkin emas. O'qituvchi sifatida, AT darslarida xavfsizlik ko'nikmalarini shakllantirish, pedagogik va texnik choralarni uyg'un qo'llash muhimdir. Shu bilan birga, kiberxavfsizlik bo'yicha doimiy trening va nazorat samarali natija beradi. Kelajakda kasbiy faoliyatda AT va axborot xavfsizligi integratsiyasi yanada kengayadi.

ADABIYOTLAR RO'YXATI

1. Smith J. *Information Technology in Professional Activities*. New York: TechPress, 2020.
2. Brown A. *Cybersecurity Threats in Modern Workplaces*. London: CyberPub, 2021.
3. Johnson L. *Fundamentals of Information Security*. Boston: InfoSec Books, 2019.
4. Davis R., Clark P. *Integrating IT into Education*. Cambridge: EduTech, 2022.
5. Miller T. *Professional Use of Information Technology*. Oxford: ITPress, 2020.
6. Wilson H. *Teaching Cybersecurity Competencies*. Berlin: Springer, 2021.