TA’LIM MUASSASALARIDA KIBERXAVFSIZLIK CHORALARI.

Nazarov Toshpo’lat Boshbek o’g’li

Pedagogika psixologiya fakulteti Maktab menejmenti kafedrasi o’qituvchisi

Suyundikov Temurbek G’ani o’g’li

Pedagogika psixologiya fakulteti Maktab menejmenti yo’nalishi II kurs talabasi

Umarov Savronbek Xudoyberdiyevich

Pedagogika psixologiya fakulteti Maktab menejmenti yo’nalishi II kurs talabasi

Annotatsiya: Ta’lim o’qituvchilari o’quvchilarga yanada samarali ta’lim berish uchun kiber dunyodan foydalanadi. Bunda kiberxavfsizlik choralarini e’tibordan chetda qoldirmaslik zarur. O’qituvchilar, talabalar, o’quvchilar, maktab ma’muriyatining ma’lumotlari kibertahdidlardan himoyalangan bo’ lishi va ularning maxfiyligini ta’minlash uchun zarur choralar qo’llanilishi lozim.

Abstract: Education teachers use the cyber world to teach students more effectively. It is necessary not to neglect cyber security measures. Information of teachers, students, pupils, school administration should be protected from cyber threats and necessary measures should be taken to ensure their confidentiality.

Аннотация: Преподаватели образования используют кибермир для более эффективного обучения учащихся. Необходимо не пренебрегать мерами кибербезопасности. Информация учителей, учащихся, учеников, администрации школы должна быть защищена от киберугроз и должны быть приняты необходимые меры для обеспечения ее конфиденциальности.

Kalit so’zlar: Kiberxavfsizlik, maxfiylik, kiberhujum, xavfsizlik.

Keywords: Cyber security, privacy, cyber attack, security.

Ключевые слова: Кибербезопасность, конфиденциальность, кибератака, безопасность.

Kirish: Hozirgi vaqtda oliy ta’lim muassasalarida ko’plab o’qitish usullari mavjud bo’lib, ular yagona maqsadni ya’ni talabalar tomonidan bilimlarni yaxshi o’zlashtirilishini ko’zlaydilar. Onlayn ta’lim jarayonida kiberpedagogika talabalar qayerda yashashidan va komoyuterga qanday kirishidan qat’iu nazar, sifatli ta’lim olishga kissa qo’shadi. Interaktiv mahsulotlarning bunday tizimlari ilg’or kompyuter texnologiyalari asosida ta’limning mavjudligi, uzluksizligi va yuqori sifatini ta’minlashga qaratilgan. Kiberpedagogika interaktiv dasturiy ta’minot bilan birgalikda o’quv fanlarini o’qitishning sifati jihatidan yangi samarali modelini yaratish imkonini beradi. Ta’lim muassasalarida paydo bo’lgan zamonaviy interaktiv doskalar esa samarali elektron ta’lim modelini joriy etishning samaralitexnik vositasi sanaladi. Ulardan foydalanish bilan o’qitish haqiqatan ham qiziqarli bo’ladi. Masalan, interfaol doska dars tezligini tezlashtirish va unga butun auditoriyani jalb qilish imkonini beradi. Interfaol doskaning ko’rinishi talabalarning diqqatini jamlash va to’plashning foydali usuli hisoblanadi. Elektron doska talabalarga doskadagi qo’rquvni yengishga yordam beradi. Ularni o’quv jarayoniga oson jalb qiladi. Auditoriyadagi talabalar befarq qolmaydi hamda darslar oson va qiziqarli o’tadi.

Asosiy qism: Kiberxavfsizlik butun mamlakat bo'ylab ta'lim muassasalarini tashvishga solmoqda. Garchi ko'p odamlar xavfsizlik tahdidlarini faqat onlayn universitetlar va muassasalar uchun xavf deb o'ylashlari mumkin bo'lsa-da, haqiqat shundaki, hamma maqsadli. Mahalliy boshlang'ich maktab, davlat universiteti yoki onlayn ta'lim portali bo'ladimi, kiber tahdidlar jiddiy zarar etkazishi mumkin.So'nggi o'n yil ichida kiberxavfsizlik juda ko'p yutuqlarga erishdi. Ma'lumotni saqlash va almashishning xavfsizroq usullari bilan biz to'g'ri yo'nalishda ketayapmiz.Biroq, faqat o'qituvchilar, talabalar va qaror qabul qiluvchilarni kiberxavfsizlik tahdidlari haqida o'rgatishning o'zi etarli emas. Har bir inson onlaynda xavfsiz bo'lib qolishi uchun amalda bo'ladigan jarayonlar va strategiyalar bo'lishi kerak. Kiberxavfsizlik raqamli muhitda maxfiy ma'lumotlarni qanday qilib xavfsiz saqlash haqida. Ta'lim muassasalarida quyidagi

ma'lumotlar haqida gap ketganda maxfiylik va maxfiylikni ta'minlash kerak bo'lgan juda ko'p turli sohalar bo'ladi:

- Talabalar va o'qituvchilarning shaxsiy aloqa ma'lumotlari;
- Tashkilot tomonidan ishlatilishi mumkin bo'lgan moliyaviy ma'lumotlar va onlayn hisoblar;
- Ushbu muassasa uchun qat'iy maxfiy va shaxsiy bo'lgan ichki operatsion ma'lumotlar va jarayonlar;
- O'quv materiallarini boshqarish uchun foydalaniladigan boshqa ma'lumotlar (ayniqsa, topshiriqlar, imtihonlar va baholash nuqtai nazaridan).

Tashkilotga xos bo'lgan sohalarga qo'shimcha ravishda, shaxsiy ma'lumotlar ham xavf ostida bo'lishi mumkin. Agar har qanday shaxsiy akkauntlardan talabalar va o'qituvchilar tomonidan institutsional qurilmalarda onlayn foydalanilsa, ular ham yomon niyatli tajovuzkorlar tomonidan foydalanishlari mumkin. Ta'lim muassasasi uchun asosiy tahdidlar ma'lumotlar xavfsizligi o'z ichiga oladi. Bular quyidagilardan iborat:

Hack: Ruxsatsiz kompyuter tizimi/tarmoqqa kirish, natijada maxfiy ma'lumotlarni o'g'irlash yoki tizimlarga zarar yetkazish. Masalan, xakerlar universitet ma'lumotlar bazasiga kirib, xodimlarning shaxsiy ma'lumotlarini o'g'irlashlari va pul mablag'larini o'g'irlash uchun shaxsiy moliyaviy hisoblariga kirishlari mumkin.

Phishing: Buzg'unchilar elektron pochta, soxta veb-saytlar yoki hatto matnlardan foydalanib, odamlarni aldash uchun parollar yoki kredit karta raqamlari kabi nozik ma'lumotlarni ochib berishadi. Soxta to‘lov havolalari yoki schyot-fakturalar korxonalar va ta’lim muassasalariga nisbatan qo‘llaniladigan eng keng tarqalgan fishing hujumlaridan biridir.

Ma'lumotlarning buzilishi: Maxfiy ma'lumotlarni (masalan, shaxsiy/moliyaviy ma'lumotlarni) o'g'irlash, ishlatish yoki oshkor qilish.

Zararli dastur: Muassasa tarmog'i yoki tizimiga zarar yetkazuvchi zararli dastur. Bularga troyanlar, viruslar va qurilmalarga zarar yetkazadigan, ularni yaroqsiz holga keltiradigan to'lov dasturlari kiradi.

MitM hujumlari: Bu "o'rtadagi odam" hujumlari bo'lib, bu erda aloqalar ushlanadi va ikki tomon o'rtasida yuborilgan ma'lumotlar tajovuzkor tomonidan o'zgartiriladi.Ta'limda kiberxavfsizlik bo'yicha eng yaxshi amaliyotlardan ba'zilari quyidagilarni o'z ichiga oladi:

-kuchli parollarni joriy qilish;

-dasturiy ta'minot va xavfsizlik tizimlarini muntazam yangilab turish;

-xavfsizlik bo'yicha treninglarni targ'ib qilish;

-kirishni cheklash[1].

Kiberxavfsizlikni fundamental atamalarini aniqlashga turli yondashuvlar mavjud. Xususan ba’zi mutaxassislar kiberxavfsizlikka oid atamalarga quyidagicha ta’rif berishgan:

Konfidensiallik - axborot yoki uni eltuvchining shunday holati bo’lib, undan ruxsatsiz tanishishning yoki nusxalashning oldi olingan bo’ladi. Konfidensiallik axborotni ruxsatsiz “o’qish”dan himoyalash bilan shug’ullanadi. Ayniqsa, bank sistemasida bank uchun konfidensiallik juda muhim.

Risk - potensial foyda yoki zarar bo’lib, umumiy holda har qanday vaziyatga biror bir hodisani yuzaga kelish ehtimoli qo’shilganida risk paydo bo’ladi. ISO “risk – bu noaniqlikning maqsadlarga ta’siri” sifatida ta’rif bergan.

kibermakon — axborot texnologiyalari yordamida yaratilgan virtual muhit;

kibertahdid — kibermakonda shaxs, jamiyat va davlat manfaatlariga tahdid soluvchi shart-sharoitlar va omillar majmui;

kiberxavfsizlik — kibermakonda shaxs, jamiyat va davlat manfaatlarining tashqi va ichki tahdidlardan himoyalanganlik holati;

[1] .https://www.thelearningapps.com/uz/cybersecurity-in-education-going-beyond-security-awareness/

kiberxavfsizlik hodisasi — kibermakonda axborot tizimlarining ishlashida uzilishlarga va (yoki) ulardagi axborotning ochiqligi, yaxlitligi va undan erkin foydalanilishining buzilishiga olib kelgan hodisa;

kiberxavfsizlik obyekti — axborotning kiberhimoya qilinishini hamda milliy axborot tizimlari va resurslarining kiberxavfsizligini ta’minlashga doir faoliyatda foydalaniladigan axborot tizimlari majmui, shu jumladan muhim axborot infratuzilmasi obyektlari;

kiberxavfsizlik subyekti — milliy axborot resurslariga ega bo‘lish, ulardan foydalanish va ularni tasarruf etish hamda ulardan foydalanish bo‘yicha elektron axborot xizmatlari ko‘rsatish, axborotni himoya qilish hamda kiberxavfsizlik bilan bog‘liq muayyan huquqlar va majburiyatlarga ega bo‘lgan yuridik shaxs va (yoki) yakka tartibdagi tadbirkor, shu jumladan muhim axborot infratuzilmasi subyektlari;

kiberhimoya — kiberxavfsizlik hodisalarining oldini olishga, kiberhujumlarni aniqlashga va ulardan himoya qilishga, kiberhujumlarning oqibatlarini bartaraf etishga, telekommunikatsiya tarmoqlari, axborot tizimlari hamda resurslari faoliyatining barqarorligini va ishonchliligini tiklashga qaratilgan huquqiy, tashkiliy, moliyaviy-iqtisodiy, muhandislik-texnik chora-tadbirlar, shuningdek ma’lumotlarni kriptografik va texnik jihatdan himoya qilish chora-tadbirlari majmui;

kiberhujum — kibermakonda apparat, apparat-dasturiy va dasturiy vositalardan foydalangan holda qasddan amalga oshiriladigan, kiberxavfsizlikka tahdid soladigan harakat[2].

Xulosa: Ta'lim organlari hodisalarni kuzatish va kiberhujumlarning oldini olish uchun monitoring va tergov choralarini ko'rishlari kerak. Tarmoq trafigini kuzatish, zaifliklarni aniqlash va ularga javob berish uchun kiberxavfsizlik guruhi samarali tashkil etilishi kerak. Ushbu jamoa mumkin bo'lgan tahdidlarni kuzatishi va kerak bo'lganda ehtiyot choralarini ko'rishi mumkin.Kiberxavfsizlik kun sayin ta'lim masalalari uchun

[2] https://lex.uz/uz/docs/-5960604

muhimroq bo'lib bormoqda. Ma'lumotlar xavfsizligi va maxfiylikning buzilishi ham o'quvchilar, ham maktab obro'si uchun jiddiy oqibatlarga olib kelishi mumkin. Shu sababli, ta'lim muassaslari doimo kiberxavfsizlikdan xabardor bo'lishlari, tegishli ehtiyot choralarini ko'rishlari va xavfsiz qolish uchun xavfsizlik siyosatlarining qat'iy bajarilishini ta'minlashlari kerak.

Foydalanilgan adabiyotlar:

1.https://www.thelearningapps.com/uz/cybersecurity-in-education-going-beyond-security-awareness/

2.https://lex.uz/uz/docs/-5960604