AXBOROT XAVFSIZLIGIGA BO‘LADIGAN TAHDIDLAR

UMAROV NURIDDIN

Uchquduq tuman 1-sonli politexnikum maxsus fan o‘qituvchisi

Fan: Axborot xavfsizligi

ANNOTATSIYA

Ushbu maqolada axborot xavfsizligiga bo‘layotgan zamonaviy tahdidlar, ularning kelib chiqish sabablari va ularni oldini olish bo‘yicha amaliy choralar yoritilgan. Dasturiy tahdidlar, ijtimoiy muhitdagi firibgarliklar, kiberhujumlar, ma’lumotlarni o‘g‘irlash va ichki xatarlar kabi xavf turlari tahlil qilinadi. Shuningdek, tashkilotlar va foydalanuvchilar uchun samarali himoya strategiyalari, zamonaviy texnologik vositalardan foydalanish yo‘llari ko‘rib chiqiladi. Maqola axborot xavfsizligini ta’minlashga doir amaliy yondashuvlarni o‘rganishga qaratilgan bo‘lib, real muammolar va ularning yechimlariga e’tibor qaratadi.

Kalit so‘zlar: *Axborot xavfsizligi, kiberxavf, tahdid, ma’lumotlarni himoyalash, kiberhujum, zararli dastur, firibgarlik, xavfsizlik strategiyasi.*

KIRISH

Raqamli texnologiyalar hayotimizning ajralmas qismiga aylangan bir davrda axborot xavfsizligini ta'minlash dolzarb masalaga aylandi. Bugungi kunda nafaqat yirik tashkilotlar, balki har bir oddiy foydalanuvchi ham o‘z ma’lumotlarini himoya qilish zaruriyatiga duch kelmoqda. Kiberxavfsizlik sohasida yuzaga kelayotgan yangi tahdidlar zararli dasturlar, ma'lumotlarni o‘g‘irlash, ijtimoiy muhitdagi firibgarliklar va ichki xatarlar axborot resurslarini himoya qilish choralarini yangilab borishni talab qilmoqda.

Axborot xavfsizligiga tahdidlar turli shakllarda namoyon bo‘lib, ular nafaqat texnik vositalar orqali, balki ijtimoiy muhit va inson omili orqali ham amalga oshirilmoqda. Aynan shuning uchun ushbu mavzuni chuqur tahlil qilish,

tahdidlarning turlari va ularni kamaytirish yo‘llarini amaliy nuqtayi nazardan ko‘rib chiqish juda muhimdir.

Ushbu maqola zamonaviy tahdidlar mohiyatini yoritish, ularning manbalarini aniqlash va axborot xavfsizligini ta'minlashga qaratilgan amaliy choralarni tahlil qilishga qaratilgan.

ASOSIY QISM

Axborot xavfsizligiga tahdidlarni kamaytirish uchun har bir tashkilot va foydalanuvchi kundalik faoliyatida aniq va oddiy xavfsizlik qoidalariga amal qilishi lozim. Masalan, parollarni faqat son va harflardan emas, balki maxsus belgilar ishtirokida yaratish, ularni har oyda yangilab turish eng sodda, ammo samarali himoya chorasidir. Bir xil parolni bir nechta tizimda ishlatish esa kiberjinoyatchilar uchun imkoniyat eshigini ochadi.

Ish muhitida elektron pochta orqali kelgan shubhali xatlarni ochmaslik, ilovalarga ko‘r-ko‘rona ishonmaslik zarur. Amaliy tarzda bu xatlarni yuboruvchisiga telefon orqali qo‘ng‘iroq qilib tasdiqlash orqali tekshirish mumkin. Ko‘plab firibgarliklar aynan ishonuvchanlik orqali sodir bo‘lmoqda. Xodimlarga bu borada muntazam treninglar o‘tkazish foydali bo‘ladi. Trening davomida ular real vaziyatlarda qanday harakat qilishni rolli o‘yinlar yordamida o‘rganadilar.

Kiberxavfsizlikni kuchaytirish uchun antivirus dasturlarini doimiy ravishda yangilab borish va avtomatik tekshiruv rejimlarini yoqib qo‘yish muhim.

Korxonalar o‘z serverlarini zaxira nusxalari bilan himoyalashi, ya'ni ma'lumotlarni haftalik rejimda boshqa joyga ko‘chirib borishi zarur. Bu amaliy yondashuv kutilmagan texnik muammolar yoki hujumlar paytida axborotni yo‘qotmaslikka yordam beradi.

Jamoat Wi-Fi tarmoqlarida shaxsiy hisobga kirish, masalan, bank ilovalaridan foydalanish xavf tug‘diradi. Shu sababli foydalanuvchilarga VPN dasturlaridan foydalanish tavsiya qilinadi. Bu ilova ularning trafik ma'lumotlarini shifrlab, tashqi tahdidlar oldini oladi.

Ichki xatarlar ham e’tibordan chetda qolmasligi kerak. Har bir tashkilotda kirish huquqlari qat’iy belgilanishi, ya’ni kim qanday fayllarga ruxsatga ega ekani aniq bo‘lishi lozim. Shaxsiy fleshkalardan foydalangan holda kompaniya kompyuterlariga zararli dasturlar tushishi mumkin. Shu sababli barcha tashqi qurilmalarni avtomatik tekshiruvdan o‘tkazuvchi tizimlar joriy etilishi kerak.

Tashkilotlar o‘z xodimlari orasida axborot xavfsizligi madaniyatini shakllantirishi zarur. Bu, masalan, devorlarda oddiy eslatmalar, tizimga kirishda xavfsizlik haqida qisqa ogohlantirishlar orqali amalga oshirilishi mumkin. Amaliy jihatdan qaraganda, kichik eslatmalar ham foydalanuvchilarning hushyorligini oshiradi.

Axborotni shifrlash eng ishonchli himoya usullaridan biri. Masalan, muhim hujjatlar shifrlangan fayl shaklida saqlansa, hatto ular o‘g‘irlangan taqdirda ham ulardan foydalanish imkoni bo‘lmaydi. Shifrlash dasturlaridan foydalanishni barcha xodimlar bilishi va ulardan samarali foydalana olishi kerak.

Axborot xavfsizligiga doir kreativ va amaliy misollar jadvali

Tahdid turi	**Amaliy holat (misol)**	**Amaliy yechim (kreativ yondashuv)**
Shubhali e-mail xabarlari	Xodim “rahbardan” kelgan hujjatni ochib, virusli faylni ishga tushirib yuboradi.	Har bir xodimga “real va soxta emailni farqlash” bo‘yicha mini-treninglar o'tkazish.
Zaif parol ishlatilishi	Foydalanuvchi parol sifatida 123456 dan foydalanadi, tizimga osongina kirish mumkin.	Parollarni avtomatik kuchli formatda yaratadigan va har 30 kunda yangilaydigan tizim joriy qilish.

Tahdid turi	Amaliy holat (misol)	Amaliy yechim (kreativ yondashuv)
Jamoat Wi-Fi tarmog‘i orqali hujum	Xodim kafe Wi-Fi tarmog‘ida bank hisobiga kiradi va ma’lumotlari o‘g‘irlanadi.	Korxona barcha xodimlarga bepul VPN ilovasini o‘rnatib beradi va undan foydalanishni majburiy qiladi.
Ichki xodim tomonidan tahdid	Ishdan ketayotgan xodim maxfiy fayllarni ko‘chirib oladi.	Har bir foydalanuvchining kirish huquqlari qat’iy cheklanadi, ishdan ketgan zahoti avtomatik bloklanadi.
USB orqali virus kirishi	Xodim o‘z fleshkasini ulab, tasodifan virusli faylni kompyuterga o‘tkazadi.	Tashqi qurilmalar avtomatik skanerdan o‘tadigan filtr o‘rnatiladi, ruxsatsiz qurilmalar bloklanadi.
Foydalanuvchi bexabarligi	Yangi ish boshlagan xodim zararli linkni bosadi.	Ishga kirgan kuniyoq “axborot xavfsizligi 10 qoidasi” bo‘yicha interaktiv o‘yin tarzida o‘rgatish.
Hujjatlarni umumiy joyda saqlash	Muhim ma’lumotlar umumiy papkada turadi va hamma foydalanuvchi ularga kira oladi.	Muhim fayllar uchun shifrlangan, parol bilan himoyalangan papkalar yaratish.
Avtomatik yangilanish yo‘qligi	Kompyuterda eski antivirus ishlaydi, yangi tahdidlarga qarshi zaif.	Antiviruslar va operatsion tizimlar avtomatik tarzda yangilanishi yo‘lga qo‘yiladi.

XULOSA

Zamonaviy texnologiyalar kundalik hayotimizni yengillashtirayotgani bilan birga, axborot xavfsizligiga oid tahdidlar ham tobora murakkablashib bormoqda.

Ushbu tahdidlarning oldini olish faqat texnik vositalarga emas, balki foydalanuvchilarning xabardorligi va amaliy ehtiyot choralariga ham bog‘liq. Har bir foydalanuvchi oddiy profilaktik qoidalarga amal qilsa, ko‘plab xavflarning oldini olish mumkin.

Kompaniyalar esa o‘z axborot tizimlarini nafaqat tashqi tahdidlardan, balki ichki xatar manbalaridan ham himoya qiluvchi, real sharoitlarga moslangan xavfsizlik siyosatini ishlab chiqishi zarur. Har bir texnologik vosita inson tomonidan boshqariladi, shuning uchun inson omilini e’tibordan chetda qoldirmaslik muvaffaqiyatli axborot xavfsizligining asosiy garovidir.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. Rasulov, O. (2020). Axborot xavfsizligi asoslari. Toshkent: Innovatsion texnologiyalar nashriyoti.

2. Xudoyberdiyev, M. (2019). Kompyuter tizimlarida axborotni himoyalash. Toshkent: Fan va texnologiya.

3. Mamatqulov, A. (2021). Kiberxavfsizlik va raqamli tahdidlar. Samarqand: SamDU nashriyoti.

4. Usmonov, Sh. (2022). Axborot texnologiyalari va xavfsizlik. Toshkent: Iqtisod-Moliya nashriyoti.

5. Jo‘rayev, N. (2018). Elektron hukumat va axborot xavfsizligi. Toshkent: Yangi asr avlodi.