AXBOROTNI RUXSATSIZ FOYDALANISHLARDAN HIMOYALASH.

Israyiljanova Gulbaxor Saminjanovna
TATU Farg'ona filiali akademik litseyi
Umarov Abdumuxtor Maxammad o'g'li
TATU Farg'ona filiali

Annotatsiya. *Axborot foydalanishiga qarshi himoyalashning zarurati va muhimligi, ruxsatsiz foydalanishning axborot tarmog'iga qanday tahdidlar olib kelishi mumkinligini va ushbu tahdidlarni oldini olish uchun qanday qadamga o'tilishi kerakligini ko'rsatadi. Undan tashqari kompyuterlar, mobil qurilmalar, tarmoq qurilmalari va internet xizmatlarini himoya qilish uchun muhim texnologiyalarni o'z ichiga oladi.*

Kalit so'z. *Ruxsatsiz foydalanish, himoya, tahdidlar, tarmoq xavfsizligi, ishonchsizlik, tarmoq monitoring, foydalanuvchi haqiqiyligi, xavfsizlik sozlamalari, maxfiylik, ruxsatsiz kiritish.*

Axborot - huquq ob'ektidir. Kompyuter jinoyatchiligi uchun asboblar sifatida telekommunikasiya va hisoblash texnikasi vositalari, dastur ta'minoti va intellektual bilimlar, ularni mukammallashgan sohalari nafaqatgina kompyuterlar, korporativ va global tarmoqlargina bo'lib kolmasdan, balki zamonaviy yuqori axborot texnologiyalari vositalari ishlatiladigan, katta xajmdagi axborotlar qayta ishlanadigan, masalan, statistika va moliya institutlari, faoliyatni istalgan sohasi bo'lishlari mumkin.

Zamonaviy kompaniyalar o'zlarining ixtiyorida katta miqdordagi ma'lumotlarga ega. Bugungi voqelikda bu asosiy resursdir. Ma'lumotlar bazalari kompaniya faoliyati va mavjudligi uchun jiddiy xavf tug'diradigan jinoiy foydalanishdan ishonchli himoyalangan bo'lishi kerak. Shuning uchun ma'lumotlarni ruxsatsiz kirishdan himoya qilishni ta'minlash juda muhimdir. Bu foydalanuvchi vakolatlarini nazorat qilishga qaratilgan chora-tadbirlar majmuidir. Kompaniya xodimlarning bevosita vazifalarini bajarishi kerak bo'lmagan ma'lumotlardan foydalanishga cheklovlar kiritadi. Qog'oz hujjatlar bilan ham, elektron tashuvchilardagi ma'lumotlar bilan ham harakatlarni nazorat qilish kerak.

Ishonchli axborot xavfsizligi tizimini yaratish uchun siz ma'lumotlarni olishning mumkin bo'lgan usullarini aniqlashingiz kerak.

Chet elliklar uchun ma'lumotlarga kirish usullari

Axborotga ruxsatsiz kirish (axborotga ruxsatsiz kirish) turli usullar bilan olinishi mumkin. Hujjatlarni to'g'ridan-to'g'ri o'g'irlash yoki kompyuter operatsion tizimlarini buzish variantlarning faqat kichik bir qismidir. Axborotni saqlashning elektron vositalari eng zaif hisoblanadi, chunki ularni masofaviy boshqarish va boshqarish usullaridan foydalanish mumkin.

Noqonuniy kirishni olishning mumkin bo'lgan variantlari:

aloqa tizimlariga ulanish (telefon liniyalari, interkomlar, simli interkomlar);

hujjatlarni o'g'irlash, shu jumladan dushmanlik maqsadlarida nusxa ko'chirish (ko'paytirish);

kompyuterlar, tashqi disklar yoki ma'lumotni o'z ichiga olgan boshqa qurilmalardan bevosita foydalanish;

Internet orqali operatsion tizimga joriy etish, shu jumladan josuslik dasturlari, viruslar va boshqa zararli dasturlardan foydalanish;

axborot manbalari sifatida kompaniya xodimlaridan (insayderlardan) foydalanish.

Gartner ma'lumotlariga ko'ra, odamlarning 60 foizi vaziyat bo'yinturug'i ostida jinoyat qilishga tayyor. Sizning xodimlaringiz SearchInform ProfileCenter-dan qanday foydalanishga qodirligini bilib oling.

Faol aloqa kanaliga ulanish ma'lumotlar bazalariga to'g'ridan-to'g'ri kirishsiz, bilvosita ma'lumot olish imkonini beradi. Optik tolali liniyalar tashqi kirishdan eng himoyalangan hisoblanadi, ammo ular ba'zi tayyorgarlik operatsiyalaridan keyin ham birlashtirilishi mumkin. Bunday holda, hujumchilarning maqsadi xodimlarning ishchi muzokaralari - masalan, tergov tadbirlari paytida yoki moliyaviy operatsiyalarni amalga oshirishda. Ruxsatsiz kirish himoya tizimidagi har qanday xatolikdan foydalanadi va himoya vositalarining irratsional tanlovi, ularning noto'g'ri o'rnatilishi va konfiguratsiyasi bilan mumkin.

Ma'lumotni o'g'irlash, o'zgartirish yoki yo'q qilish mumkin bo'lgan buzish kanallarining tasnifi

1. Shaxs orqali:

• axborot tashuvchilarni o'g'irlash;

• ekran yoki klaviaturadan ma'lumotlarni o'qish; • chop etilgan ma'lumotni o'qish.

2. Dastur orqali:

• parollarni ushlash;

• shifrlangan axborotning shifrini ochish;

• tashuvchidan ma'lumotlarni nusxalash.

3. Uskunalar orqali:

• axborotga kirishni ta'minlovchi maxsus ishlab chiqilgan texnik vositalarni ulash;

• uskunalar, aloqa liniyalari, elektr ta'minoti tarmoqlari va boshqalardan soxta elektromagnit nurlanishni ushlab turish.

Kompyuterda ishlash jarayonida ko‘pincha ma’lumotlardan birini yoki boshqasini noqonunuy, ruxsatsiz ko‘rish va tahrirlashdan himoya qilish kerak. Ushbu vazifa odatda lokal tarmoqda ishlayotganda, shuningdek turli vaqtlarda bir nechta foydalanuvchilar kompyuterdan foydalana olganda paydo bo‘ladi.

FOYDALANILGAN ADABIYOTLAR.

1. Umarov, A., & Ro‘zaliyev, A. (2023). AXBOROTNI RUXSATSIZ FOYDALANISHLARDAN HIMOYALASH. Educational Research in Universal Sciences, 2(11), 500–502

2. Ro‘zaliyev Abdumalikjon Vahobjon o’g’li, Umarov Abdumuxtor Maxammad o‘g‘li, & R. Adaxanov. (2022). AXBOROT XAVFSIZLIGIDA BIOMETRIK HIMOYA USULLARI. Proceedings of International Educators Conference, 1(2), 177–181.

3. Muxtorov Farrux Muxammadovich, Umarov Abdumuxtor Maxammad o’g’li, & Ro’zaliyev Abdumalikjon Vahobjon o’g’li. (2022). Умаров , А.

4. Umarov, A., & Qutlug'beka, T. (2023). FISHING HUJUMLARDAN HIMOYA QILISHNING ASOSIY USULLARI VA CHORALARI. INNOVATION IN THE MODERN EDUCATION SYSTEM, 3(36), 317-320.

5. Muxtarov, F., Umarov, A., & Ro’zaliyev, A. (2023). Axborot tizimlarida xavfsizlik tahdidlarining tasnifi. Engineering problems and innovations.

6. Makhmudov, I. A., & Isroiljonova, G. S. (2021). The package multiservice services in NGN. Academic research in educational sciences, 2(6), 989-994.

7. Karimov, SH. T., & Israyiljanova, G. S. (2023). YURAK URISH TEZLIGINING OZGARUVCHANLIGINI ORGANISH. INNOVATION IN THE MODERN EDUCATION SYSTEM, 3(30), 389-395.