AXBOROTNI RUXSATSIZ FOYDALANISHLARDAN HIMOYALASH

Umarov Abdumuxtor, Ro‘zaliyev Abdumalikjon
TATU Farg‘ona filiali

ANNOTATSIYA

Ushbu maqola ma’lumotlarni ruxsatsiz kirish va foydalanishdan himoya qilish uchun qo‘llaniladigan usullar va strategiyalar haqida qisqacha ma’lumot beradi. Texnik va tashkiliy jihatlar, shuningdek, maxfiy ma’lumotlar va axborot resurslarini samarali himoya qilish uchun zarur bo‘lgan asosiy vositalar va amaliy tavsiyalar muhokama qilinadi. Ushbu mavzu o‘zlarining axborot infratuzilmasi ishonchliligini ta’minlashga intilayotgan shaxslar uchun ham, tashkilotlar uchun ham katta ahamiyatga ega. Ushbu maqolada biz ma’lumotlarni ruxsatsiz foydalanishdan himoya qilishning asosiy jihatlarini ko‘rib chiqamiz.

Kalit so‘zlar: Axborot xavfsizligi, autentifikatsiya, shifrlash, kirishni nazorat qilish, axborot xavfsizligiga tahdidlar, ma’lumotlarni himoya qilish, maxfiylik, ruxsatsiz kirish, kiberxavfsizlik.

Hozirgi dunyoda axborot shaxslar, korxonalar va hukumatlar faoliyatida muhim rol o‘ynaydi. U eng qimmatli boyliklardan biridir va shuning uchun uning xavfsizligi birinchi o‘rinda turadi. Axborotga ruxsatsiz kirish jiddiy oqibatlarga olib kelishi mumkin, jumladan, maxfiy ma’lumotlarning sizib chiqishi, obro‘siga putur yetkazish va moliyaviy yo‘qotish.

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 RO‘YXATI: (REFERENCES)

1. Umarov, A. M. O. G. L. (2021). AXBOROT XAVFSIZLIGI XAVFINI BAHOLASH. Scientific progress, 2(8), 293-300.
2. AXBOROT XAVFSIZLIGIDA BIOMETRIK HIMOYA USULLARI
3. RA Vahobjon o‘g, UA Maxammad o‘g‘li, R Adaxanov - Proceedings of International Educators Conference, 2022
4. AXBOROTNI XIMOYALASH TIZIMINI ISHLAB CHIQISH
5. MF Muxammadovich, UA Maxammad o‘g‘li - Proceedings of International Educators Conference, 2022
6. Muxtarov, F., Umarov, A., & Ro‘zaliyev, A. (2023). AXBOROT TIZIMLARIDA XAVFSIZLIK TAHDIDLARINING TASNIFI. Engineering problems and innovations.
7. “Основы зашиты”, Москва, 2020 71 b.
8. “СБОРНИК РУКОВОДЯЩИХ ДОКУМЕНТОВ ПО ЗАЩИТЕ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА”
9. https://cyberleninka.ru/article/n/axborot-xavfsizligi-xavfini-baholash