AXBOROT TIZIMLARIDAN FOYDALANISHDA AXBOROT XAVFSIZLIGINI TA'MINLASH USULLARI

Aminova Hafiza Obidovna
BMTI akademik litseyi
Informatika va axborot texnologiyalari

Annotatsiya
Axborot xavfsizligini ta'minlash. Axborot xavfsizligini ta'minlash – bu foydalanuvchining axborotlarini himoyalashga qo'yilgan me'yor va talablarni bajarishidir. Axborot xavfsizligi esa bu axborot foydalanuvchilariga va ko'plab axborot tizimlariga zarar keltiruvchi tabiiy yoki sun'iy xarakterga ega tasodifiy va uyushtirilgan ta'sirlardan axborotlarni va axborot kommunikatsiya tizim ob'ektlarining himoyalanganligidir.

Kalit so'zlar: Axborot xavfsizligi, login, kiberhujum, himoya, avtorizatsiya.

KIRISH

Login tushunchasi. Login – shaxsning, o'zini axborot kommunikatsiya tizimiga tanishtirish jarayonida qo'llaniladigan belgilar ketma-ketligi bo'lib, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo'lish uchun foydalaniluvchining maxfiy bo'lmagan qayd yozuvi hisoblanadi[1].
Parol tushunchasi. Parol – uning egasi haqiqiyligini aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi. U kompyuter bilan muloqot boshlashdan oldin, unga klaviatura yoki identifikatsiya kartasi yordamida kiritiladigan harfli, raqamli yoki harfli-raqamli kod shaklidagi mahfiy so'zdan iborat.

ASOSIY QISM

Avtorizatsiya tushunchasi. Avtorizatsiya – foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni. Bunda foydalanuvchiga hisoblash tizimida ba'zi ishlarni bajarish uchun muayyan huquqlar beriladi. Avtorizatsiya shaxs harakati doirasini va u foydalanadigan resurslarni belgilaydi.
Ro'yxatdan o'tish tartibi. Ro'yxatdan o'tish – foydalanuvchilarni ro'yxatga olish va ularga dasturlar va ma'lumotlarni ishlatishga huquq berish jarayoni. Ayrim veb-saytlar foydalanuvchilarga qo'shimcha xizmatlarni olish va pullik xizmatlarga obuna bo'lish uchun ro'yxatdan o'tishni, ya'ni o'zi haqida ayrim ma'lumotlarni kiritishni (anketa to'ldirishni) hamda login va parol olishni taklif qiladilar. Foydalanuvchi ro'yxatdan o'tgandan so'ng tizimda unga qayd yozuvi (akkount) yaratiladi va unda foydalanuvchiga tegishli axborotlar saqlanadi.

[1] S.S.Kosimov. Axborot texnologiyalari. Ukuv kullanma. - T., Aloqachi, 2016.

Login va parolga ega bo‘lish shartlari. Biror shaxs o‘zining login va paroliga ega bo‘lishi uchun u birinchidan axborot kommunikatsiya tizimida ruyxatdan o‘tgan bo‘lishi kerak va shundan so‘ng u o‘z logini va parolini o‘zi hosil qilishi yoki tizim tomonidan berilgan login parolga ega bo‘lishi mumkin. Login va parollar ma’lum uzunlikdagi belgilar ketma-ketligidan tashkil topadi. Login va parollarning uzunligi va qiyinligi uning qanchalik xavfsizligini ya’ni buzib bo‘lmasligini ta’minlaydi.

Fishing – ijtimoiy injeneriyaning bir turi bo‘lib, foydalanuvchilarning tarmoq xavfsizligi asoslarini bilmasligiga asoslangan. Jumladan, ko‘pchilik oddiy faktni bilishmaydi: servislar qayd yozuvingiz ma’lumotlari, parol va shu kabi ma’lumotlarni yuborishni so‘rab hech qachon xat yubormaydi[2].

Resurslardan ruxsatsiz foydalanish va uning oqibatlari. Axborot-kommunikatsiya tizimining ixtiyoriy tarkibiy qismlaridan biri bo‘lgan hamda axborot tizimi taqdim etadigan imkoniyat mavjud bo‘lgan resurslardan belgilangan qoidalarga muvofiq bo‘lmagan holda foydalanishni cheklash qoidalariga rioya qilmasdan foydalanish – bu resurslardan ruxsatsiz foydalanish toifasiga kiradi. Bunday foydalanish natijasida quyidagi oqibatlar yuzaga kelishi mumkin:

- axborotning o‘g‘irlanishi;
- axborotni o‘zgartirish;
- axborotning yo‘qotilishi;
- yolg‘on axborotni kiritish;
- axborotni qalbakilashtirish va h.k.

Viruslarning turlari va vazifalari. Viruslarni quyidagi asosiy alomatlari bo‘yicha turkumlash mumkin:

- yashash makoni;
- operatsion tizim;
- ishlash algoritmi xususiyati.

Hujum tushunchasi. Hujum tushunchasi – buzg‘unchining biror bir maqsad yo‘lida axborot kommunikatsiya tizimlarining mavjud himoyalash tizimlarini buzishga qaratilgan harakati.

Axborot hujumlari va undan saqlanish qoidalari. Axborot hujumlari odatda 3 ga bo‘linadi:

- Obyekt haqida ma’lumotlar yig‘ish (razvedkalash) hujumi.
- Obyektdan foydalanishga ruxsat olish hujumi.
- Xizmat ko‘rsatishdan voz kechish xujumi.

Axborot hujumlaridan saqlanishda birinchi navbatda axborot kommunikatsiya tizimi obyektlariga qilinayotgan hujumlarni topib olishda qo‘llaniladigan mexanizm va vositalarni qo‘llash kerak. Bularga tarmoqlararo ekran (FIREWALL) va xujumlarni aniqlash (IDS) vositalarini misol tariqasida keltirish mumkin.

[2] S.K.Yeaniev, M.M. Karimov. Xisoblash sistemalari va tarmoqlarida informatsiya ximoyasi. Oliy ukuv yurt.talab. uchun ukuv kullanma. - T,. Davlat texnika universiteti, 2013.

ADABIYOTLAR RO`YXATI

1. S.S.Kosimov. Axborot texnologiyalari. Ukuv kullanma. - T., Aloqachi, 2016.
2. S.K.Yeaniev, M.M. Karimov. Xisoblash sistemalari va tarmoqlarida informatsiya ximoyasi. Oliy ukuv yurt.talab. uchun ukuv kullanma. - T,. Davlat texnika universiteti, 2013.
3. Г.Н. Устинов. Основы Информационной безопасности систем и сетей передачи данных. Учебное пособие. Серия «Безопасность». -М.: СИНТЕГ, 2000.