ELEKTRON XAVSIZLIK TUSHUNCHASI.

Chirchiq Shahar 1-sonli texnikumi Informatika va axborot texnologiyalar fan o'qtuvchisi ***Suleymenova Rushana Asomidinovna***

Annotatsiya: *Elektr xavfsizligi vositalari va jihozlari elektr toki urishi, kuyish, yiqilish, yiqilish va hokazo kabi baxtsiz hodisalarni oldini olish va xodimlarning shaxsiy xavfsizligini ta'minlash uchun turli xil maxsus asboblar va jihozlarni nazarda tutadi.*

Umumiy himoya vositalari: xodimlarning baxtsiz hodisalarini oldini olish uchun ishlatiladigan xavfsizlik vositalari, masalan, xavfsizlik kamarlaridan, dubulg'alardan va boshqalarni nazarda tutadi, normal holatlarda oyoq tokalari, ko'tarish taxtalari, narvonlari va toqqa chiqish uchun o'tkazuvchi poyabzallari toifasi.

Xavfsizlikning asosiy vositalari va jihozlari: tok kuchi bilan ishlaydigan asboblarni to'g'ridan-to'g'ri boshqarishi yoki tegib turishi mumkin bo'lgan yoki elektr tok ko'targichlari bilan aloqa qilishi mumkin bo'lgan elektr asboblarini, masalan, sig'imli elektroskoplar, izolyatsiya tayoqchalari, yadro fazali qurilmalar, izolyatsiya qopqoqlari, izolyatsiya bo'linmalari va boshqalarni anglatadi. Va jonli ishlaydigan asboblar va asboblarning farqi shundaki, ular ish paytida qisqa vaqt davomida jonli narsalar yoki aloqa qilmaydigan jonli narsalar bilan aloqa qilishadi.

Yordamchi izolyatsiyalash xavfsizligi vositalari va jihozlari: izolyatsiya kuchi deganda va'da qilingan asbob-uskunalar yoki liniyalarning ish kuchlanishi emas, balki faqat aloqa kuchlanishi, qadam kuchlanishi, oqish oqimi oldini olish uchun asosiy xavfsizlik vositalari va jihozlarining xavfsizlik funktsiyasini kuchaytirish uchun foydalaniladi. va operatorlarga zarar etkazishdan boshq. Yordamchi izolyatsion xavfsizlik moslamalarini quyidagilar bilan ishlatmang: izolyatsiya qiluvchi qo'lqoplar, izolyatsiyalovchi etiklar, oyoq izollari va boshqalar.

Xavfsizlik belgilari: odatda turli xil xavfsizlik ogohlantiruvchi belgilar, uskunalar belgilari va hk.

Elektr xavfsizligi vositalarining keng tarqalgan turlari: umumiy himoya vositalari

Xavfsizlik zarbasi: bu xodimlar boshini himoya qilish va boshni tashqi ta'sirdan himoya qilish uchun ishlatiladigan bir xil bosh kiyimdir.

Yuqori voltli kiruvchi signalizatsiya xavfsizlik dubulg'asi: bu yuqori voltli elektrga yaqin signalizatsiya funktsiyasiga ega xavfsizlik shlemidir. Odatda, bu oddiy xavfsizlik dubulg'asi va yuqori voltli elektr energiyasiga yaqin signalizatsiya kombinatsiyasi.

Xavfsizlik kamari: Bu operatorning biznes tarmog'iga tushib qolishining oldini olish uchun ishlatiladigan shaxsiy himoya vositalari. U belbog ', ustunli belbog', metall aksessuarlar va boshqalardan iborat.

Elektr xavfsizligi uskunalarining keng tarqalgan turlari: o'rni izolyatsiyalash xavfsizligi uskunalari

Kapasitiv elektroskop / yuqori voltli elektroskop: Bu yuqori voltli elektr jihozlari va liniyalarining ish kuchlanishiga ega yoki yo'qligini&# 39 elektroskopi orqali erga o'tkazib yuborilgan oqimni aniqlash orqali tekshiradigan uskuna.

Izolyatsiya tayoqchasi: qisqa vaqt ichida ishlaydigan asbob-uskunalarni ishlatish yoki o'lchash uchun ishlatiladigan izolyatsiya vositasini, masalan, yuqori voltli izolyatsiya kalitlarini ulash yoki ajratish, sug'urta to'siqlarini tushirish va boshqalarni nazarda tutadi. odatda ishchi qismga, izolyatsion qismga va qo'l qismiga bo'linadi.

Axborot xavfsizligi (inglizcha: *Information Security*, shuningdek, inglizcha: *InfoSec*) — *axborotni ruxsatsiz kirish*, foydalanish, oshkor qilish, buzish, o‘zgartirish, tadqiq qilish, yozib olish yoki yo‘q qilishning oldini olish amaliyotidir. Ushbu universal *kontseptsiya ma’lumotlar* qanday shaklda bo‘lishidan qat’iy nazar (masalan, elektron yoki, jismoniy) amal qiladi. Axborot xavfsizligini ta’minlashning asosiy maqsadi ma’lumotlarning konfidensialligi, yaxlitligi va mavjudligini muvozanatli, qo‘llashning maqsadga muvofiqligini hisobga olgan holda va tashkilot faoliyatiga hech qanday zarar yetkazmasdan himoya qilishdir.

Bunga, birinchi navbatda, asosiy vositalar va nomoddiy aktivlar, tahdid manbalari, zaifliklar, potensial ta’sirlar va mavjud xavflarni boshqarish imkoniyatlarini aniqlaydigan ko‘p bosqichli xavflarni boshqarish jarayoni orqali erishiladi. Bu jarayon xavflarni boshqarish rejasining samaradorligini baholash bilan birga olib boriladi.

Ushbu faoliyatni *standartlashtirish* maqsadida ilmiy va kasbiy hamjamiyatlar texnik axborot xavfsizligi choralari, yuridik javobgarlik, shuningdek, foydalanuvchi va ma’murlarni tayyorlash standartlari sohasida asosiy metodologiya, siyosat va tarmoq standartlarini ishlab chiqishga qaratilgan doimiy hamkorlik asosida ish olib boradi. Ushbu standartlashtirishga asosan, ma’lumotlarga kirish, qayta ishlash, saqlash va uzatishni tartibga soluvchi keng ko‘lamli qonunlar va qoidalar ta’sir ko‘rsatadi. Biroq, tashkilotda agar doimiy takomillashtirish madaniyati to‘g‘ri shakllantirilmagan bo‘lsa, har qanday standartlar va metodologiyalarni joriy etish yuzaki ta’sir ko‘rsatishi mumkin .

Tahdidlar va xavfsizlik choralari

Axborot xavfsizligiga tahdidlar turli shakllarda bo‘lishi mumkin. 2018-yil uchun eng jiddiy tahdidlar „xizmat ko‘rsatish usulidagi jinoyatlar“ (inglizcha: *Crime-as-a-Service*), Internet mahsulotlari, ta’minot zanjirlari va tartibga solish talablarining murakkabligi bilan bog‘liq bo‘lgan tahdidlar bo‘lgan . „Xizmat ko‘rsatish usulidagi jinoyatlar“ yirik jinoiy hamjamiyatlar uchun darknet bozorida jinoiy xizmatlar paketini yangi paydo bo‘lgan kiberjinoyatchilarga arzon narxlarda taqdim etishning bir namunasidir. Bu yuqori texnik murakkablik yoki yuqori narx tufayli ilgari erishib bo‘lmagan xakerlik hujumlarini amalga oshirish imkonini beradi. Bu esa kiberjinoyatni ommaviy hodisaga aylantiradi. Ko‘pgina tashkilotlar Internet mahsulotlarini faol tatbiq qilmoqdalar. Bu qurilmalar ko‘pincha xavfsizlik talablarisiz ishlab chiqilganligi bois, kiberhujumlar uchun qo‘shimcha imkoniyatlar yaratadi. Bundan tashqari, internet xizmatlarining jadal rivojlanishi va murakkablashuvi uning shaffofligini pasaytiradi, bu esa noaniq belgilangan huquqiy qoidalar va shartlar bilan birgalikda tashkilotlarga qurilmalar tomonidan to‘plangan

mijozlarning shaxsiy ma’lumotlaridan o‘z ixtiyoriga ko‘ra, ular bilmagan holda foydalanish imkonini beradi. Bundan tashqari, tashkilotlarning o‘zlari IoT qurilmalari tomonidan to‘plangan ma’lumotlarning qaysi biri tashqariga uzatilishini kuzatishi mushkul masaladir. Ta’minot zanjirlariga tahdid shundaki, tashkilotlar o‘zlarining yetkazib beruvchilari bilan turli xil qimmatli va nozik ma’lumotlarni almashishadi, natijada ular ustidan bevosita nazorat yo‘qoladi. Shunday qilib, ushbu ma’lumotlarning maxfiyligi, yaxlitligi yoki mavjudligini buzish xavfi sezilarli darajada oshadi. Bugungi kunda regulyatorlarning tobora ko‘payib borayotgan yangi talablari tashkilotlarning hayotiy axborot aktivlarini boshqarishni sezilarli darajada murakkablashtirmoqda. Masalan, 2018-yilda Yevropa Ittifoqida qabul qilingan „Umumiy ma’lumotlarni himoya qilish qoidalari“ (inglizcha: *General Data Protection Regulation, GDPR*) har qanday tashkilotdan istalgan vaqtda o‘z faoliyati yoki ta’minot zanjirining istalgan qismida joylashtirilgan shaxsiy ma’lumotlarning mazmuni, ularni qayta ishlash usullari, saqlanish va himoyalanish tartibi va qanday maqsadlar uchun xizmat qilishini ko‘rsatishni talab qiladi. Bundan tashqari, ushbu ma’lumot nafaqat vakolatli organlar tomonidan tekshirish paytida, balki ushbu ma’lumotlar egasining birinchi talabiga binoan ham taqdim etilishi lozim. Bunday muvofiqlikka rioya qilish muhim byudjet mablag‘lari va resurslarini tashkilotning boshqa axborot xavfsizligi vazifalaridan chetlashtirishni talab qiladi. Shaxsiy ma’lumotlarni qayta ishlashni soddalashtirish uzoq muddatli istiqbolda axborot xavfsizligini yaxshilashni nazarda tutsa ham, qisqa muddatda tashkilotning xatarlari sezilarli darajada oshadi.

Aksariyat odamlar u yoki bu tarzda axborot xavfsizligi tahdidlariga duchor bo‘lishadi. Masalan, ular zararli dasturlar (viruslar va kompyuter qurti, troya oti(kompyuter virusi) va firibgarlik dasturlari), fishing yoki identifikatorni o‘g‘irlash qurboni bo‘lishadi. Fishing (inglizcha: *Phishing*) — maxfiy ma’lumotlarni (masalan, hisob, parol yoki kredit karta ma’lumotlari) olishga qaratilgan firibgarlik harakatlaridir. Odatda, ular internet foydalanuvchisini har qanday tashkilotning (bank, internet-do‘kon, ijtimoiy tarmoq va hokazo) asl veb-saytidan ajratib

bo‘lmaydigan soxta veb-saytga jalb qilishga harakat qiladilar. Qoida tariqasida, bunday urinishlar tashkilot nomidan soxta veb-saytlarga havolalarni o‘z ichiga olgan soxta elektron pochta xabarlarini ommaviy yuborish orqali amalga oshiriladi. Foydalanuvchi brauzerda bunday havolani ochib, o‘z hisob ma’lumotlarini kiritib firibgarlarning o‘ljasiga aylanadi . 1964-yilda[18] ingliz tiliga **Turkcha:** atamasi „Identifikatsiya o‘g‘irligi“ kiritilgan bo‘lib, unda kimningdir shaxsiy ma’lumotlari (masalan, ko‘pincha fishing yo‘li bilan olingan ism, bank hisobi yoki kredit karta raqami) firibgarlik va boshqa jinoyatlarni sodir etishda foydalaniladi. Jinoyatchilar nomidan noqonuniy moliyaviy imtiyozlar, qarz olgan yoki boshqa jinoyatlarni sodir etgan shaxs ko‘pincha ayblanuvchining o‘zi bo‘lib qoladi va bu uning uchun jiddiy moliyaviy va huquqiy oqibatlarga olib kelishi mumkin. Axborot xavfsizligi shaxsiy hayotga bevosita ta’sir qiladi va bu holat turli madaniyatlarda turlicha ta’riflanishi mumkin.

Hukumatlar, harbiylar, korporatsiyalar, moliya institutlari, tibbiyot muassasalari va xususiy korxonalar o‘z xodimlari, mijozlari, mahsulotlari, tadqiqotlari va moliyaviy natijalari haqida doimiy ravishda katta miqdordagi maxfiy ma’lumotlarni to‘playdi. Agar bunday ma’lumotlar raqobatchilar yoki kiberjinoyatchilar qo‘liga tushib qolsa, bu tashkilot va uning mijozlari uchun keng qamrovli huquqiy oqibatlarga, tuzatib bo‘lmas moliyaviy va ayanchli yo‘qotishlarga olib kelishi mumkin. Biznes nuqtai nazaridan, axborot xavfsizligi xarajatlarga nisbatan muvozanatli bo‘lishi kerak. Gordon-Lob[en] iqtisodiy modeli bu muammoni hal qilishning matematik apparatni tavsiflaydi. Unga ko‘ra axborot xavfsizligi tahdidlari yoki axborot xavflariga qarshi kurashishning asosiy usullari quyidagilardan iborat:

- *kamaytirish* — zaifliklarni bartaraf etish va tahdidlarning oldini olish uchun xavfsizlik va qarshi choralarni amalga oshirish;
- *uzatish* — tahdidlarni amalga oshirish bilan bog‘liq xarajatlarni uchinchi shaxslar: sug‘urta yoki autsorsing kompaniyalariga o‘tkazish;

- *qabul qilish* — xavfsizlik choralarini amalga oshirish xarajatlari tahdidni amalga oshirishdan mumkin bo‘lgan zarardan oshib ketgan taqdirda moliyaviy zaxiralarni shakllantirish;
- *voz kechish* — haddan tashqari xavfli faoliyatdan voz kechish.

FOYDALANILGAN ADABIYOTLAR:

1.www.tdpu.uz – Nizomiy nomidagi TDPU rasmiy sayti 2.www.ziyonet.uz – ZiyoNet axborot ta’lim portal 3.www.edu.uz – O‘zbekiston Respublikasi Oliy va o‘rta maxsus ta’lim vazirligi https://scientific-jl.com/luch/ 428 Часть-43_ Том-2_ Апрел-2025 portali 4.http://www.ctc.msiu.ru/materials/Book1,2/index1.html 5.http://www.ctc.msiu.ru/materials/CS_Book/A5_book.tgz 6.Qosimov S.S. Axborot texnologiyalari. – T.: Aloqachi, 2006 – 369 b. 7.Iskusstvenniy intellekt: Sovremennie podxodi – A Rassel i Norvig. – iz. Pirson Prentice Hall