RAQAMLI IQTISOD MA'LUMOTLARINI XIMOYALASH USULLARINING QO'LLANILISH SOXALARI.

Abdumajitova Ziyodaxon Xajiakbar qizi - Guliston davlat universiteti Amaliy matematika yo'nalishi 4 bosqich talabasi

Annotatsiya: Bu maqola raqamli iqtisod ma'lumotlarini ximoyalash usullarining qo'llanilish soxalari haqida ma'lumot beradi. Maqolada raqamli iqtisodiy ma'lumotlar, ularning ximoyalash usullari va bu usullarni qo'llashning muhimligi haqida tushunchalar beriladi. Maqola ilmiy tadqiqotlarga asoslangan bo'lib, raqamli iqtisodiy ma'lumotlarini to'plash, tahlil qilish va ximoyalashning qanday amaliyotlar orqali bajarilishi haqida ma'lumotlar beriladi.

Kalit so'zlar: Login, parol, avtorizatsiya, kompyuter virusi, hujum tushunchasi.

Axborot xavfsizligini ta'minlash. Axborot xavfsizligini ta'minlash – bu foydalanuvchining axborotlarini himoyalashga quyilgan 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.

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.

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.

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 [1].

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 (account) yaratiladi va unda foydalanuvchiga tegishli axborotlar saqlanadi [2].

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.

Login va parolni buzish. Login va parolni buzish – bu buzg‘unchining biror bir maqsad yo‘lida axborot kommunikatsiya tizimi ob’ektlaridan foydalanish uchun qonuniy tarzda foydalanuvchilarga tegishli login va parollarini buzishdir. Bunda maxsus dastur yordamida login va parollar generatsiya qilib topiladi. Login va parollarning uzunligi bu jarayonning uzoq vaqt davom etishiga yoki generatsiya qilaolmasiligiga ishora bo‘ladi [3].

Login va parolni o‘g‘irlash. Login va parolni o‘g‘irlash – bu foydalanuvchilarning mahfiy ma’lumotlari bo‘lgan login va parollarga ega bo‘lish maqsadida amalga oshiriladigan internet firibgarligining bir turidir. Bu mashhur brendlar, masalan, ijtimoiy tarmoqlar, banklar va boshqa servislar nomidan elektron xatlarni ommaviy jo‘natish yo‘li orqali amalga oshiriladi. Xatda odatda tashqi ko‘rinishi asl saytdan farq qilmaydigan saytga to‘g‘ri ishorat mavjud bo‘ladi. Bunday saytga tashrif buyurgan foydalanuvchi firibgarga akkauntlar va bank hisob raqamlariga kira olishga ega bo‘lishga imkon beruvchi muhim ma’lumotlarni bildirishi mumkin. 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 [4].

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:

1. axborotning o‘g‘irlanishi;
2. axborotni o‘zgartirish;
3. axborotning yo‘qotilishi;
4. yolg‘on axborotni kiritish;
5. axborotni qalbakilashtirish va h.k.

Kompyuter virusi. Kompyuter virusi – bu o‘z-o‘zidan ko‘payuvchi, kompyuter tarmoqlari va axborot tashuvchilari orqali erkin tarqaluvchi, hamda kompyuter va unda saqlanayotgan axborot va dasturlarga zarar yetkazuvchi dastur kodi yoki komandalar

ketma-ketligi hisoblanadi. Kompyuter viruslari quyidagi xossalarga ega: o'zidan nusxa ko'chirish, axborotdan ruxsatsiz foydalanishni amalga oshirish. U o'zining nusxalarini kompyuterlarda yoki kompyuter tarmoqlarida qayta ko'paytirib va tarqatib, hamda qonuniy foydalanuvchilar uchun nomaqbul harakatlarni bajaradi. Virus, aksariyat hollarda nosozlik va buzilishlarga sabab bo'ladi va biror hodisa yuz berishi bilan, masalan, aniq kunning kelishi bilan ishga tushirilishi mumkin. [5]

1. Viruslarning turlari va vazifalari. Viruslarni quyidagi asosiy alomatlari bo'yicha turkumlash mumkin:
2. yashash makoni;
3. operatsion tizim;
4. ishlash algoritmi xususiyati.

Kompyuter viruslarini yashash makoni, boshqacha aytganda viruslar kiritiluvchi kompyuter tizimi ob'ektlarining xili bo'yicha turkumlash asosiy va keng tarqalgan turkumlash hisoblanadi.

Fayl viruslar turli usullar bilan bajariluvchi fayllarga kiritiladi (eng ko'p tarqalgan viruslar xili), yoki fayl yo'ldoshlar (kompanon viruslar) yaratadi yoki faylli sistemalarni (link-viruslar) tashkil etish xususiyatidan foydalanadi.

Yuklama viruslar o'zini diskning yuklama sektoriga (boot - sektoriga) yoki vinchesterning tizimli yuklovchisi (Master Boot Record) bo'lgan sektorga yozadi. Yuklama viruslar tizim yuklanishida boshqarishni oluvchi dastur kodi vazifasini bajaradi.

Makroviruslar axborotni ishlovchi zamonaviy tizimlarning makrodasturlarini va fayllarini, xususan MicroSoft Word, MicroSoft Excel va h. kabi ommaviy muharrirlarning fayl-xujjatlarini va elektron jadvallarini zaharlaydi.

Tarmoq viruslari o'zini tarqatishda kompyuter tarmoqlari va elektron pochta protokollari va komandalaridan foydalanadi. Ba'zida tarmoq viruslarini "qurt" xilidagi dasturlar deb yuritishadi. Tarmoq viruslari Internet-qurtlarga (Internet bo'yicha tarqaladi), IRC-qurtlarga (chatlar, Internet Relay Chat) bo'linadi.

Kompyuter viruslarining vazifalari, odatda, to'rt bosqichni o'z ichiga oladi:

1. virusni xotiraga yuklash;
2. qurbonni qidirish;
3. topilgan qurbonni zaharlash;
4. destruktiv funksiyalarni bajarish.

Viruslarga qarshi kurashish usullari. Hozirgi kunda kompyuter viruslarini aniqlash va ulardan himoyalanish uchun maxsus dasturlarning bir necha xillari ishlab chiqilgan bo'lib bu dasturlar kompyuter viruslarini aniqlash va yo'qotishga imkon beradi. Bunday dasturlar virusga qarshi dasturlar yoki antiviruslar deb yuritiladi. Antivirus dasturlariga AVP, Doctorweb, Nod32 dasturlarini kiritish mumkin. Umuman

barcha virusga qarshi dasturlar zaharlangan dasturlar va yuklama sektorlarning avtomatik tarzda tiklanishini ta'minlaydi [6,7].

1. Viruslarga qarshi kurashishning asosan quyidagi usullari mavjud:
2. Muntazam profilaktika ishlarini, ya'ni virusga tekshiruv ishlarini olib borish.
3. Taniqli virusni zararsizlantirish.
4. Taniqli bo'lmagan virusni zarasizlantirish.

Hujum tushunchasi. Xujum tushunchasi – buzg'unchining biror bir maqsad yo'lida axborot kommunikatsiya tizimlarining mavjud himoyalash tizimlarini buzishga qaratilgan harakati [8].

Axborot xujumlari va undan saklanish qoidalari. Axborot hujumlari odatda 3 ga bo'linadi:

1. Ob'ekt haqida ma'lumotlar yig'ish (razvedkalash) hujumi.
2. Ob'ektdan foydalanishga ruxsat olish hujumi.
3. Xizmat ko'rsatishdan voz kechish xujumi.

Axborot xujumlaridan saqlanishda birinchi navbatda axborot kommunikatsiya tizimi ob'ektlariga 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.

Foydalanilgan adabiyotlar:

1. Jo'ravayev A.A. O'zaro ma'lumot almashuvchi idoralar o'rtasida kalitlarni boshqarish. Studencheskiy vestnik, № 20(165), 82-84 b.

2. Gunjan Srivastava, J. N. Singh & Manisha Manjul (2021) Group key management: Issues and opportunities, Journal of Discrete Mathematical Sciences and Cryptography, 24:3, 787-795, DOI: 10.1080/09720529.2020.1794518

3. Akbarov D. YE. Axborot xavfsizligini ta'minlashning kriptografik usullari va ularning kullanilishi: Toshkent - «O'zbekiston markasi» nashriyoti - 2009.

4. N. A. W. Kbean and S. B. Sadkhan, "A Survey on Key management for SCADA," 2020 6th International Engineering Conference "Sustainable Technology and Development" (IEC), 2020, pp. 97-102, doi: 10.1109/IEC49899.2020.9122853.

5. A.V. Kabulov, Sh.T.Boltayev I.M.Saymanov. Zadacha sinteza upravlyayuщego agregata dlya realizatsii algoritmov informatsionnoy bezopasnosti i kriptografii. // Sbornik statey Mejdunarodnoy nauchno-prakticheskoy konferensii. - Penza: Izd-vo MSNS «Nauka i prosveщeniye», 2018, S. 75-79.

6. Lipayev V. V. Sistemnoye proyektirovaniye slojnыx programmnыx sredstv dlya informatsionnыx sistem Sinteg; 268 str., 2002 g.

7. OpenScience. Blokcheyn. Stoit li doveryat novoy texnologii. UzAcademia. Xesh funksiyalar

8. A.P. Alferov, A.Yu. Zubov, A.S. Kuzmin, A.V. Cheremushkin Artem Semenovich Genkin Aleksey A. Mixeyev Blokcheyn: Kak eto rabotayet i chto jdet nas zavtra