UDK. 004

AXBOROT XAVFSIZLIGI MUAMMOLARI

Mallaboyev Nosirjon Murodullayevich
NamMQI, katta o‘qituvchi, +998936927006, mnosirjon07@gmail.com

Dadamirzayev Muzaffar G’ulomqodirovich
NamMQI, katta o‘qituvchi, +998 99 436 77 55muzaffardadamir81@gmail.com

Annotatsiya: Ushbu maqolada kompyuter tizimi va tarmoqlarida axborotlarni himoyalash vositalari, havf xatarlar va hujum turlari, konkret tashkiliy, texnikaviy yoki uskunaviy, dasturiy, huquqiy, jismoniy, kriptografik, kompyuter tarmoqlarining aloqa kanallarida axborotlarni himoyalash va viruslardan himoyalash vositalari keng yoritilib berilgan. Turli xildagi axborotlar hududiy joylashishidan qat’iy nazar bizning kundalik hayotimizga Internet xalqaro kompyuter tarmogi orqali kirib keldi. Axborotlashgan jamiyat shu kompyuter tarmog‘i orqali tezlik bilan shakllanib bormoqda. Axborotlar dunyosiga sayohat qilishda davlat chegaralari degan tushuncha yo‘qolib bormoqda. Jahon kompyuter tarmog‘i davlat boshqaruvini tubdan o‘zgartirmoqda, ya’ni davlat axborotlaring tarqalishi mexanizmini boshqarishdagi muammolari hamda zamonaviy kompyuter tizimlarini yaratilishi va global axborot tarmoqlarini paydo bo‘lishi axborotni himoya qilish muammolari batafsil yoritib berilgan.

Аннотация: В данной статье рассмотрены средства защиты информации в компьютерных системах и сетях, угрозы и виды атак, специфические организационные, технические или аппаратные, программные, правовые, физические, криптографические, средства защиты информации в каналах связи компьютерных сетей и защиты от вирусов широко освещаются. Различные виды информации вошли в нашу повседневную жизнь через международную компьютерную сеть Интернет, независимо от географического положения. Благодаря этой компьютерной сети быстро формируется информационное общество. Понятие государственных границ исчезает при путешествии в мир информации. Глобальная компьютерная сеть коренным образом меняет государственное управление, то есть подробно разъясняются проблемы управления механизмом распространения публичной информации, а также создание современных компьютерных систем и появление глобальных информационных сетей, проблемы защиты информации.

Annotation: This article discusses the means of protecting information in computer systems and networks, threats and types of attacks, specific organizational, technical or hardware, software, legal, physical, cryptographic, means of protecting information in communication channels of computer networks and protecting against viruses are widely covered. Various types of information have entered our daily life through the international computer network Internet, regardless of geographical location. Thanks to this computer network, the information society is rapidly emerging. The concept of state borders disappears when traveling into the world of information. The global computer network radically changes public administration, that is, the problems of managing the mechanism for disseminating public information, as well as the creation of modern computer systems and the emergence of global information networks, and the problems of information security are explained in detail.

Kalit so‘zlar: kompyuter, texnologiya, internet, biometrik, onlayn, konfidentsial, elektron, texnik, sertifikat, administrator, resurs, versiya, blok, brandmauer.

Ключевые слова: компьютер, технология, интернет, биометрический, онлайн, конфиденциальный, электронный, технический, сертификат, администратор, ресурс, версия, блокировка, брандмауэр.

Key words: computer, technology, internet, biometric, online, confidential, electronic, technical, certificate, administrator, resource, version, blocking, firewall.

Yaqin o‘tgan yillarda, Kompyuter texnologiyalari hayotimizga chuqur singib ketgan. Bizning zamonamizda odamlar kompyutersiz qanday ishlaganliklarini tasavvur qilishlari juda qiyin, ular ularga juda ko‘nikib qolgan. Kompyuterlar mavjudligi bilan odamlar Internet - elektron pochta, World Wide Web, Internet-banking xizmatlaridan ham faol foydalana boshladilar. Endi, oddiy odamning har kuni ertalab yangiliklar lentasini standart ko‘rish, shaxsiy pochta mazmunini tekshirish, turli mashhur ijtimoiy tarmoqlarga tashrif buyurish, onlayn-do‘konlarda xarid qilish, turli xizmatlar uchun haq to‘lash. bilan boshlanadi. Internet asta-sekin, lekin shubhasiz aylandi. kundalik ishlarimizda doimiy yordamchi. Internet muloqotni osonlashtiradi va til to‘siqlarini yo‘q qiladi, endi sizning do‘stingiz sizdan ming kilometr uzoqda boshqa shaharda yoki hatto boshqa davlatda yashasa ham, agar xohlasangiz, u bilan hech bo‘lmaganda kun bo‘yi muloqot qilishingiz mumkin. Ammo Internetning barcha afzalliklari bilan birga, u juda ko‘p xavf-xatarlarni ham o‘z ichiga oladi. Avvalo, bu shaxsiy va davlat xavfsizligiga tahdiddir. Internet-bu shaxsiy ma’lumotlar, bank kartalari ma’lumotlarini osongina o‘g’irlash mumkin bo‘lgan, Internetda axborot urushlari olib boriladigan, ma’lumot to‘qnashuvlari yuzaga keladigan bo‘sh joy.

Shunday qilib, axborot xavfsizligiga tahdid eng muhim muammolardan biridir zamonaviy hayot inson va biz bu qaerdan kelib chiqqanligini va o‘zimizni qanday himoya qilishimiz mumkinligini bilishimiz kerak.

Zamonaviy jamiyat hayotini zamonaviy axborot texnologiyalarisiz tasavvur qilib bo‘lmaydi. Kompyuterlar bank tizimlariga xizmat qiladi, yadro reaktorlarining ishlashini nazorat qiladi, energiyani taqsimlaydi, poezdlar jadvalini nazorat qiladi, samolyotlarni, kosmik kemalarni boshqaradi. Kompyuter tarmoqlari va telekommunikatsiyalar mamlakat mudofaa va xavfsizlik tizimlarining ishonchliligi va imkoniyatlarini oldindan belgilab beradi. Kompyuterlar axborotni saqlash, uni qayta ishlash va iste’molchilarga taqdim etishni ta’minlaydi, shu bilan axborot texnologiyalarini joriy qiladi. Biroq, aynan yuqori darajadagi avtomatlashtirish xavfsizlikni (shaxsiy, axborot, davlat va boshqalar) kamaytirish xavfini keltirib chiqaradi. Axborot texnologiyalari va kompyuterlarning mavjudligi va keng qo‘llanilishi ularni buzg’unchi ta’sirlarga juda zaif qiladi. Bunga ko‘plab misollar keltirish mumkin[1].

Ostida **axborot xavfsizligiga tahdid** axborot resurslari, shu jumladan saqlanadigan, uzatiladigan va qayta ishlangan axborotni, shuningdek, dasturiy va texnik vositalarni yo‘q qilish, buzish yoki ruxsatsiz foydalanishga olib kelishi mumkin bo‘lgan harakat yoki hodisani anglatadi.

Internet texnologiyalarining yaratilishi turli manbalardan tez va oson yo‘l bilan axborot olish imkoniyatlarini hamma uchun-oddiy fuqarodan tortib yirik tashkilotlargacha misli ko‘rilmagan darajada oshirib yubordi. Davlat muassasalari, fan-ta’lim muassasalari, tijorat korxonalari va alohida shaxslar axborotni elektron shaklda yaratib-saqlay boshladilar. Bu muhit avvalgi fizikaviy saqlashga nisbatan katta qulayliklar tug’diradi: saqlash juda ixcham, uzatish esa bir onda yuz beradi va tarmoq orqali boy ma’lumotlar bazalariga murojaat qilish imkoniyatlari juda keng. Axborotdan samarali foydalanish imkoniyatlari axborot miqdorining tez ko‘payishiga olib keldi. Biznes qator tijorat sohalarida bugun axborotni o‘zining eng qimmatli mulki deb biladi. Bu albatta ommaviy axborot va hamma bilishi mumkin bo‘lgan axborot haqida gap borganda o‘ta ijobiy hodisa. Lekin pinhona (konfidentsial) va maxfiy axborot oqimlari uchun Internet texnologiyalari qulayliklar bilan bir qatorda yangi muammolar keltirib chiqardi. Internet muhitida axborot xavfsizligiga tahdid keskin oshdi. AQSH dagi kompyuter xavfsizligi instituti va FBR tomonidan kompyuter jinoyatlari bo‘yicha 1999 yilda o‘tkazilgan so‘rov natijalariga ko‘ra so‘rovda qatnashgan tashkilotlarning 57 foyizi Internet bilan ulanish joyi "ko‘pincha tajovuzlar tashkil etiladigan joy" deb, 30 foyizi ularning tarmog’iga suqulib kirish yuz berganini,

26 foyizi esa tajovuz vaqtida pinhona axborotni o‘g’irlash sodir bo‘lganini ma’lum qilishgan. AQSH kompyuter jinoyatlariga qarshi kurash Federal markazi-FedCIRC ma’lumotlariga ko‘ra 1998 yilda 1100000 kompyuterli 130000 ga yaqin davlat tarmoqlari tajovuzga duchor bo‘lgan. "Kompyuter tajovuzi" deganda kishilar tomonidan kompyuterga beruxsat kirish uchun maxsus dasturni ishga tushirishni nazarda tutiladi. Bunday tajovuzlarni tashkil etish shakllari har xil. Ular quyidagi turlarga bo‘linadi.[2]. Kompyuterga olisdan kirish: Internet yoki intranetga kimligini bildirmay kirishga imkon beruvchi dasturlar. O‘zi ishlab turgan kompyuterga kirish: kompyuterga kimligini bildirmay kirish dasturlari asosida. Kompyuterni olisdan turib ishlatmay qo‘yish: Internet (yo tarmoq) orqali olisdan kompyuterga ulanib, uning yoki uni ayrim dasturlarining ishlashini to‘xtatib qo‘yuvchi dasturlar asosida (ishlatib yuborish uchun kompyuterni qayta ishga solish yetarli). O‘zi ishlab turgan kompyuterni ishlatmay qo‘yish: ishlatmay qo‘yuvchi dasturlar vositasida. Tarmoq skanerlari: tarmoqda ishlayotgan kompyuter va dasturlardan qay biri tajovuzga chidamsizligini aniqlash maqsadida tarmoq haqiqatda axborot yig’uvchi dasturlar vositasida. Dasturlarning tajovuzga bo‘sh joylarini topish: Internetdagi kompyuterlarning katta guruhlari orasidan tajovuzga bardoshsizlarini izlab qarab chiquvchi dasturlar vositasida. Parol ochish: parollar fayllaridan oson topiladigan parollarni izlovchi dasturlar vositasida. Tarmoq tahlilchilari (snifferlar): tarmoq trafikini tinglovchi dasturlar vositasida. Ularda foydalanuvchilarning nomlarini, parollarini, kredit kartalari nomerlarini trafikdan avtomatik tarzda ajratib olish imkoniyati mavjud. Ma’lumotlar massivini jo‘natuvchi tomonidan uni jo‘natganligini yoki oluvchi tomonidan uni olganligini tan olishdan bo‘yin tovlashining oldini olish. Ko‘plab qo‘shimcha xizmatlar (audit, kirishni ta’minlash) va qo‘llab-quvvatlash xizmatlari (kalitlarni boshqarish, xavfsizlikni ta’minlash, tarmoqni boshqarish) mazkur asosiy xavfsizlik tizimini to‘ldirishga xizmat qiladi. Web tugunining to‘la xavfsizlik tizimi barcha yuqorida keltirilgan xavfsizlik yo‘nalishlarini qamrab olgan bo‘lishi shart. Bunda tegishli xavfsizlik vositalari (mexanizmlari) dasturiy mahsulotlar tarkibiga kiritilgan bo‘lishi lozim. Autentifikatsiyalashni takomillashtirish qayta ishlatiladigan parollarga xos kamchiliklarni bartaraf etishni, shu maqsadda bir martagina ishlatiladigan parol tizimidan tortib identifikatsiyalashning yuqori texnologik biometrik tizimlarigacha qo‘llashni nazarda tutadi. Foydalanuvchilar o‘zlari bilan olib yuradigan predmetlar, masalan, maxsus kartochkalar, maxsus jeton yoki disketa ancha arzon ham xavfsiz[3]. Noyob, modul kodi himoyalangan dastur moduli ham bu maqsadlarda qulay. Oshkor kalitlar infratuzilmasi ham Web–tugun xavfsizligining ajralmas qismi. Autentifikatsiya, ma’lumot butunligi va axborot pinhonalig i(konfidentsialligi)ni ta’minlash uchun ishlatiladigan taqsimlashga n tizim(odamlar, kompyuterlar), Ochiq kalit infrastrukturali (sertifikat nashrchisi) elektron sertifikatni e’lon qiladi. Unda foydalanuvchi identifikatori, uning ochiq kaliti, xavfsizlik tizimi uchun qandaydir qo‘shimcha axborot va sertifikat nashr etuvchisining raqamli imzosi bor. Ideal variantda bu tizim Yer yuzining har qanday ikki nuqtasidagi foydalanuvchi uchun sertifikatlar zanjirini tuzib beradi. Bu zanjircha kimgadir maxfiy xatni imzolash, hisob bo‘yicha pul o‘tkazish yoki elektron kontrakt tuzish uchun, boshqa kishi uchun–hujjat manbaini va imzolovchi shaxsning aslini tekshirib bilish imkonini beradi. NIST bir necha boshqa tashkilotlar bilan bu yo‘nalishda ish olib bormoqda. Internetga ulangan tarmoqlar xakerlarning tajovuzi tufayli ochiq muloqotga halal bersa ham brandmauerlar o‘rnatib oldilar. PGP ga o‘xshash mukammal dasturlar bo‘lmaganda ochiq tarmoq bo‘lishi ham mumkin bo‘lmas edi.

Tarmoqni kompyuter tajovuzlaridan himoyalash doimiy va o‘z-o‘zidan yechilmaydigan masaladir. Lekin qator oddiy himoya vositalari yordamida tarmoqqa suqulib kirishlarning ko‘pchiligini oldini olish mumkin. Masalan yaxshi konfiguratsiyalangan tarmoqlararo ekran va harbir ish stantsiyalari (kompyuterlar)da o‘rnatilgan virusga qarshi dasturlar ko‘pchilik kompyuter tajovuzlarini barbod etadi. Quyida Intranetni himoyalash bo‘yicha 14 amaliy tavsiya

bayon etilgan. Xavfsizlik siyosati lo‘nda va aniq qo‘yilishi lozim. Intranet tarmog’i xavfsizligi bo‘yicha yorqin va sobit qadamlik bilan qo‘yilisini ta’minlaydigan qoidalar va amallar bo‘lishi lozim. Tarmoq xavfsizligi tizimi uning eng bo‘sh joyi qanchalik kuchli himoyalangan bo‘lsa shu qadar kuchlidir. Agar bir tashkilot doirasida turli xavfsizlik siyosatlariga ega bo‘lgan bir necha tarmoq mavjud bo‘lsa bir tarmoq boshqa tarmoqning yomon xavfsizligi tufayli obro‘sini yo‘qotishi mumkin. Tashkilotlar shunday xavfsizlik siyosatini qabul qilishlari lozimki, kutilgan himoya darajasi hamma yerda bir xil amalga oshsin. Siyosatning eng ahamiyatli tomoni brandmauerlar orqali o‘tkaziladigan trafiklarga yagona talab ishlab chiqilishidir [4]. Shuningdek siyosat tarmoqda qaysi himoya vositalari (masalan, tajovuzlarni payqash vositalarimi yoki qaltis joylar skanerlarimi)va ular qanaqa ishlatilishi lozimligini belgilashi, yagona xavfsizlik darajasiga erishish uchun kompyuterlarning har xil turlari uchun standart xavfsiz konfiguratsiyalar belgilanishi shart. Brandmauer (Tarmoqlararo ekran, inglizcha-firewalls,) qo‘llash lozim. Bu tashkilotning eng asosiy himoya vositasidir. Tarmoqqa kiruvchi, undan chiquvchi trafik (axborot oqimi)ni nazorat qiladi. U trafikning biror turini to‘sib qo‘yishi yo tekshirib turishi mumkin. Yaxshi konfiguratsiyalangan bradmauer kompyuter tajovuzlarining ko‘pchiligini qaytarishi mumkin. brandmauerlar, intellektual kartalar va boshqa texnikaviy-dasturiy himoya vositalaridan oqilona foydalanish lozim. Brandmauer va WWW-serverlarni ularning ishini to‘xtatib qo‘yish tahdidlariga qarshi bardoshliligini testdan o‘tkazib turish lozim. Internetda kompyuterning ishini to‘xtatib qo‘yishga yo‘naltirilgan tajovuzlar tarqalgan. Tajovuzkorlar doimo WWW-saytlarni ishdan chiqaradilar, kompyuterlarni ortiq vazifalar bilan yuklab qo‘yadilar yoki tarmoqlarni ma’nosiz paketlar bilan to‘ldirib tashlaydilar. Bu turdagi tajovuzlar juda jiddiy bo‘lishi mumkin, ayniqsa tajovuzkor davomli tajovuzlarni uyushtirish darajasida aqlli bo‘lsa. Chunki buning manbaini topib bo‘lmaydi. Xavfsizligi haqida qayg’iruvchi tarmoqlar bunday tajovuzlardan ko‘riladigan zararni chamalab ko‘rish uchun o‘zlariga o‘zlari tajovuzlarni uyushtirishlari mumkin. Bunday tahlillarni faqat katta tajribaga ega tizim administratorlari yoki maxsus maslahatchilar o‘tkazishi maqsadga muvofiq.[5]. Kriptotizimlardan keng foydalanish lozim. Tajovuzkorlar ko‘pincha tarmoqqa uning ahamiyatga molik joylaridan o‘tuvchi trafigini tinglash orqali trafikdan foydalanuvchilarni va ularning parollarini ajratib olish yordamida suqulib kiradilar. Shuning uchun olisdagi mashinalar bilan bog’lanishlar parol bilan himoyalanganda shifrlanishi shart. Bu ayniqsa, bog’lanish Internet kanallari orqali amalga oshirilganda yoki ahamiyatli server bilan bog’lanilganda zarur. TCP/IP trafigini shifrlash uchun tijoratli va bepul dasturlar mavjud. Bulardan foydalanish tajovuzlarning oldini oladi. Internet muhit bilan birlashgan Intranetda axborot oqimini va resurslarni eng ishonchli himoyalash vositasi– nosimmetrik va simmetrik kriptotizimlardan birgalikda foydalanishdir. Kompyuterlarni xavfsizlik nuqtai-nazaridan savodxonlarcha konfiguratsiyalash kerak. Kompyuterda amal tizimlari yangitdan o‘rnatilganda ko‘pincha tajovuzlarga qaltis bo‘ladilar. Buning sababi amal tizimi dastlab o‘rnatilganda barcha tarmoq vositalaridan foydalanishga ruhsat beriladi va ulardan to‘g’ri foydalaniladi deb bo‘lmaydi. Bu tajovuzkor uchun mashinaga tajovuz uyushtirishda ko‘p usullardan foydalanishga yo‘l ochadi. Shuning uchun barcha zarur bo‘lmagan tarmoq vositalari kompyuterdan uzib qo‘yilishi lozim. Dasturiy ta’minotga tuzatishlarni operativ kiritishni tartibga solish (Patching). Kompaniyalar bot-bot o‘z dasturlarida topilgan xatolarni yo‘qotish uchun tuzatishlar kiritib boradilar. Agar bu xatolar tuzatilmasa tajovuzkor undan foydalanib dasturingizga va u orqali kompyuteringizga tajovuz uyushtirishi mumkin. Tizim administratorlari avvalo o‘zlarining eng zarur tizimlaridagi dasturlarga tuzatishlarni o‘rnatib zarur xostlarni himoyalashlari zarur. Chunki tuzatishlar tez-tez yuzaga kelib turadi va ularni barcha kompyuterlarda o‘rnatib chiqishga ulgurmay qolish mumkin. Odatda tuzatishlar faqat dastur ishlab chiqargan korxonadangina olinishi shart. Intranet-tarmoq xavfsizligida uchratilgan defektlarni albatta tuzatish lozim.

Qanday manbalar axborot xavfsizligiga tahdid soladi degan savol tug'ilishi tabiiy.

Agar biz axborot xavfsizligini himoya qilishni chetlab o'tadigan tahdidlar tasnifini tavsiflasak, unda bir nechta sinflarni ajratish mumkin. Sinflar tushunchasi majburiydir, chunki u barcha omillarni istisnosiz soddalashtiradi va tizimlashtiradi. Asos quyidagi kabi parametrlarni o'z ichiga oladi:

1. Axborot xavfsizligi tizimiga aralashish niyatining darajasi:

axborot o'lchovida xodimlarning e'tiborsizligidan kelib chiqadigan tahdid;

firibgarlar tomonidan boshlangan tahdid va ular buni shaxsiy manfaatlar uchun qiladilar.

2. Tashqi ko'rinish xususiyatlari:

inson qo'li bilan qo'zg'atiladigan va sun'iy bo'lgan axborot xavfsizligiga tahdid;

axborot xavfsizligi tizimlarining nazorati ostida bo'lmagan va tabiiy ofatlar natijasida yuzaga keladigan tabiiy xavflar.

3. Tahdidning bevosita sababini tasniflash. Aybdor bo'lishi mumkin:

kompaniya xodimlariga pora berish orqali maxfiy ma'lumotlarni oshkor qilgan shaxs;

falokat yoki mahalliy ofat shaklida keladigan tabiiy omil;

maxsus qurilmalardan foydalangan holda dasturiy ta'minot yoki tizimning ishlashini buzadigan texnik jihozlarga zararli kodni kiritish;

ma'lumotlarning tasodifiy o'chirilishi, vakolatli dasturiy ta'minot va apparat fondlari, operatsion tizimning ishlamay qolishi.

4. Axborot resurslariga tahdidlarning faollik darajasi:

- axborot makonida ma'lumotlarni qayta ishlash vaqtida (virus utilitlaridan pochta jo'natmalari harakati);
- yangi ma'lumotlarni olish vaqtida;
- axborotni saqlash tizimining faoliyatidan qat'i nazar (axborot ma'lumotlarini shifrlarni ochish yoki kripto himoya qilishda).

Axborot xavfsizligiga tahdid manbalarining yana bir tasnifi mavjud. U boshqa parametrlarga asoslanadi va tizimdagi nosozlik yoki buzishni tahlil qilishda ham hisobga olinadi. Bir nechta ko'rsatkichlar hisobga olinadi.

Axborot xavfsizligiga tahdidlar quyidagi holatlarda namoyon bo'ladi:

Kompyuter ma'lumotlarini yo'q qilish-bu kompyuter xotirasida uni o'chirish, uni jismoniy tashuvchilardan o'chirish, shuningdek, tarkibni tubdan o'zgartiradigan uning tarkibiy ma'lumotlariga ruxsatsiz o'zgartirishlar (masalan, noto'g'ri ma'lumotlarni kiritish, yozuvlarni qo'shish, o'zgartirish, o'chirish). Axborotni bir vaqtning o'zida boshqa mashina tashuvchisiga o'tkazish, agar ushbu harakatlar natijasida qonuniy foydalanuvchilarning ma'lumotlarga kirishiga sezilarli darajada to'sqinlik qilmasa yoki istisno etilmagan bo'lsa, jinoyat qonuni kontekstida kompyuter ma'lumotlarini yo'q qilish deb hisoblanmaydi. .

Asboblar yordamida foydalanuvchining yo'q qilingan ma'lumotlarni qayta tiklash qobiliyati dasturiy ta'minot yoki ushbu ma'lumotni boshqa foydalanuvchidan olish aybdorni javobgarlikdan ozod qilmaydi.

Axborotni yo'q qilish-bu faylning nomini o'zgartirish emas, balki u joylashgan joyda, shuningdek, avtomatik ravishda ";o'chirish"; fayllarning eski versiyalari eng so'nggi hisoblanadi.

Kompyuter ma'lumotlarini bloklash-bu foydalanuvchilarning kompyuter ma'lumotlariga kirishidagi sun'iy qiyinchilik, uni yo'q qilish bilan bog'liq bo'lmagan. Boshqacha qilib aytadigan bo'lsak, bu ma'lumotlar bilan harakatlarni bajarish, uning natijasi ma'lumotlarning o'zi to'liq xavfsizligi bilan uni maqsadli maqsadlarda olish yoki undan foydalanishning mumkin emasligi.

Axborot murosasi, qoida tariqasida, ma'lumotlar bazasiga ruxsatsiz o'zgartirishlar kiritish orqali amalga oshiriladi, buning natijasida uning iste'molchisi undan voz kechishga yoki

oʻzgarishlarni aniqlash va haqiqiy ma’lumotni tiklash uchun qoʻshimcha harakatlar qilishga majbur boʻladi. Buzilgan ma’lumotlardan foydalangan holda, iste’molchi notoʻgʻri qarorlar qabul qilish va barcha oqibatlarga olib kelishi mumkin.[6]. Axborotni rad etish, xususan, operatsiyani (bankdagi operatsiyani) tan olmaslik ma’lumotni oluvchi yoki joʻnatuvchi tomonidan uni olish yoki joʻnatish faktlarini tan olmaslikdan iborat. Marketing faoliyati nuqtai nazaridan, bu, xususan, tomonlardan biriga tuzilgan moliyaviy shartnomalarni "; texnik jihatdan" bekor qilishga imkon beradi; yoʻl bilan, ulardan rasman voz kechmasdan va shu bilan boshqa tomonga katta zarar etkazmasdan.

Kompyuter ma’lumotlarini oʻzgartirish-bu kompyuter dasturi yoki ma’lumotlar bazasini moslashtirish bilan bogʻliq boʻlganlar bundan mustasno, unga har qanday oʻzgartirishlar kiritish. EHM uchun dastur yoki ma’lumotlar bazasini moslashtirish - "faqat foydalanuvchining ma’lum bir apparatida yoki muayyan foydalanuvchi dasturlari nazorati ostida kompyuter dasturi yoki ma’lumotlar bazasining ishlashini ta’minlash maqsadida amalga oshiriladigan oʻzgartirishlar kiritish" (1-moddaning 1-qismi). Rossiya Federatsiyasining 1992 yil 23 sentyabrdagi "Elektron kompyuterlar va ma’lumotlar bazalari uchun dasturlarni huquqiy himoya qilish toʻgʻrisida" gi qonuni;). Boshqacha qilib aytganda, bu mulk egasi yoki qonuniy foydalanuvchining ixtiyorida boʻlgan dastlab (harakat sodir boʻlgunga qadar) ma’lumotlarga nisbatan uning mazmunini oʻzgartirishni anglatadi.

Kompyuter ma’lumotlarini nusxalash- ma’lumotlar bazasining ikkinchi va keyingi nusxalarini, har qanday moddiy shakldagi fayllarni ishlab chiqarish va barqaror bosib chiqarish, shuningdek ularni mashina tashuvchisida, kompyuter xotirasida yozib olish.

Xizmatni rad etish juda muhim va keng tarqalgan tahdidni ifodalaydi, uning manbai AISning oʻzi. Bunday nosozlik, ayniqsa, abonentga resurslarni taqdim etishning kechikishi uning uchun jiddiy oqibatlarga olib kelishi mumkin boʻlgan holatlarda xavflidir. Shunday qilib, ushbu qaror hali ham samarali amalga oshirilishi mumkin boʻlgan davrda qaror qabul qilish uchun zarur boʻlgan ma’lumotlarning foydalanuvchining yoʻqligi mantiqsiz harakatlarga olib kelishi mumkin.

Yuqoridagi tahdidlarning tabiatiga koʻra, ushbu tahdidlarning oldini olishga yoki yumshatishga qaratilgan hujjat aylanishidagi ma’lumotlarning himoyasini ta’minlash vazifalari shakllantiriladi. Hujjatlashtirilgan ma’lumotlarni mumkin boʻlgan xavflardan himoya qilishning asosiy yoʻnalishi xavfsiz ish jarayonini shakllantirish va hujjatlarni qayta ishlash va saqlashda har qanday turdagi tashuvchilarda ma’lumotlar xavfsizligini ta’minlaydigan ixtisoslashtirilgan texnologik tizimdan foydalanish hisoblanadi. Shunday qilib, xavfsizlik nafaqat jinoiy hujumlardan himoyalanish, balki (ayniqsa, elektron) hujjatlar va ma’lumotlarni saqlash, shuningdek, muhim hujjatlarni himoya qilish choralari va falokatlar sodir boʻlgan taqdirda faoliyatning uzluksizligi va/yoki tiklanishini ta’minlashdir.[7,8,9]. Axborotni ishonchli himoya qilish mexanizmini yaratishda tashkiliy chora-tadbirlar muhim rol oʻynaydi, chunki maxfiy ma’lumotlardan ruxsatsiz foydalanish ehtimoli koʻp jihatdan texnik jihatlar bilan emas, balki zararli harakatlar, foydalanuvchilar yoki xavfsizlik xodimlarining beparvoligi, beparvoligi va beparvoligi bilan belgilanadi. Ushbu jihatlarning ta’sirini texnik vositalar yordamida oldini olish deyarli mumkin emas. Bu maxfiy ma’lumotlarning xavfini istisno qiladigan (yoki hech boʻlmaganda minimallashtiradigan) tashkiliy, huquqiy va tashkiliy va texnik chora-tadbirlar majmuini talab qiladi. Xodimlarning maxfiy ma’lumotlar bilan ishlashi, hujjatlar va texnik vositalarni hisobga olish, saqlash va yoʻq qilish tartibi ustidan tizimli nazoratni amalga oshirish boʻyicha ishlarni tashkil etish. Xodimlarning maxfiy ma’lumotlarga kirish tartibini, tashkilotning maxfiy hujjatlarini yaratish, hisobga olish, saqlash va yoʻq qilish tartibini tartibga soluvchi yoʻriqnoma ishlab chiqilishi kerak.

ADABIYOTLAR

1.Ozoda Abdullayeva, Nosirjon Mallaboyev Process of student self-education and its design. Vol 27 No 2 (2018): Scientific Journal of Polonia University

2. Маллабоев Н., Имамназаров Э., Абдуллаева Н, Перспективы производства продуктов питания. //"Экономика и социум" №5(48) 2018. С. 770-773

3.Маллабоев Н., Шокиров Д.Роль стандарта в производстве качественных и безопасных продуктов//Экономика и социум. -Москва, 2018.-№ 5(48) С. 773-775.

4.Mamurova Feruza Tojimatovna, Abdullayeva Nozima Khoshimovna, Mallaboyev Nosirjon. Using the "assessment" method in assessing students knowledge.//Theoretical & applied science. номер: 11(79) год: 2019 страницы:80-83.

5.N.M.Mallaboev, I.A.Xolmirzaev; Joint educational educational work of the teacher and student and methods of improving the quality of education// Экономика и социум.-Москва, 2019.-№ 6(61) С. 48-53

6. Abdullaeva N, Mamurova F, Mallaboev N. Efficiency of experimental preparation use multimedia to enlarge some questions //Экономика и социум.-Москва, 2018.-№ 5(48) С. 11-13.

7. Nosirjon Mallaboyev.Using the «assessment» method in assessing students' knowledge.//International Scientific Journal ISJ Theoretical & Applied Science Philadelphia, USA issue 11, volume 79 published November 30, 2019.

8.Mallaboyev Nosirjon Murodullayevich, Dadamirzayev Muzaffar G'ulomqodirovich, Normatov Azizbek Muhammatrizoyevich. Raqamli ta’lim muhitini shakllantirish muammolari.//Fan va jamiyatning o‘zaro ta’siri–modernizatsiya va innovatsion rivojlanish sari yo‘l xalqaro onlayn ilmiy-nazariy konferensiya. 10th june 2020-Namangan city, Uzbekistan

9. Mallaboyev Nosirjon Murodullayevich, Xolmirzayev Ilxomjon A’loxanovich. Raqamli ta'lim muhitini rivojlantirishdagi muammolar.// Fan va jamiyatning o‘zaro ta’siri–modernizatsiya va innovatsion rivojlanish sari yo‘l xalqaro onlayn ilmiy-nazariy konferensiya. 10th june 2020-Namangan city, Uzbekistan