WORLDLY KNOWLEDGE
INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCHERS
ISSN : 3030-332X IMPACT FACTOR (Research bib) – 7,293

Yo'ldoshev Shohruhbek Zokirjon o'g'li
Chirchiq davlat pedagogika universiteti,
Informatika va axborot texnologiyalari kafedrasi o'qituvchisi
E-mail: norintoshloq1997@gmail.com
Tel:97 419 19 97

LOKAL KOMPYUTER TARMOQLARIDA AXBOROTLARNI KRIPTOGRAFIK HIMOYA QILISH

Annotatsiya. Lokal kompyuter tarmoqlarida ma'lumotlarni kriptografik himoya qilish bugungi kunda eng samarali va ishonchli usullardan biri hisoblanadi. Simmetrik va assimetrik kriptografik algoritmlar yordamida ma'lumotlarning maxfiyligi, yaxlitligi va autentifikatsiyasi ta'minlanadi. Ushbu maqolada Lokal kompyuter tarmoqlarida axborotlarni kriptografik himoya qilishning keng tarqalgan usullari keltirib o'tilgan.
Kalit so'zlar: To'siq, maskalash, SKIP, DES, PGP, Simmetrik kalitli shifrlash, Assimetrik kalitli shifrlash, Gibrid shifrlash.
Абстракт. Криптографическая защита данных в локальных компьютерных сетях на сегодняшний день является одним из наиболее эффективных и надежных методов. С помощью симметричных и асимметричных криптографических алгоритмов обеспечивается конфиденциальность, целостность и аутентификация данных. В данной статье описаны распространенные методы криптографической защиты информации в локальных компьютерных сетях.
Ключевые слова: Барьер, Маскирование, SKIP, DES, PGP, Шифрование с симметричным ключом, Шифрование с асимметричным ключом, Гибридное шифрование.
Abstract. Cryptographic protection of data in local computer networks is one of the most effective and reliable methods today. With the help of symmetric and asymmetric cryptographic algorithms, confidentiality, integrity and authentication of data are ensured. This article describes common methods of cryptographic protection of information in local computer networks.
Keywords: Barrier, Masking, SKIP, DES, PGP, Symmetric Key Encryption, Asymmetric Key Encryption, Hybrid Encryption.

Bugungi raqamli davrda ma'lumotlarning xavfsizligini ta'minlash asosiy masalalardan biri hisoblanadi. Kompaniyalar va tashkilotlar o'zlarining axborot tizimlarini xavfsiz saqlash uchun turli xil himoya vositalaridan foydalanadilar. Ayniqsa, lokal kompyuter tarmoqlarida ma'lumotlarni himoya qilish dolzarb muammo hisoblanadi, chunki tarmoq orqali uzatiladigan ma'lumotlar hujumchilar tomonidan o'g'irlanishi yoki buzilishi mumkin. Bu muammoni hal qilishning samarali usullaridan biri – ma'lumotlarni kriptografik himoya qilishdir. Kompaniyalarning mahalliy tarmoqlarini himoya qilish uchun, qoida tariqasida, xavfsizlik devorlari - xavfsizlik devorlari (firewall) qo'llaniladi. Xavfsizlik devori - tarmoqni ikki qismga bo'lish imkonini beruvchi (chegara mahalliy tarmoq va Internet o'rtasida joylashgan) va paketlarni bir qismdan ikkinchisiga o'tkazish shartlarini belgilovchi qoidalar to'plamini shakllantirishga imkon beruvchi kirishni boshqarish vositasi. Ekranlar ham apparat, ham dasturiy ta'minotda amalga oshirilishi mumkin.

Kompyuter tarmoqlarida axborotni himoya qilish texnologiyalarining to'plangan tajribasi shuni ko'rsatadiki, faqat axborotni himoya qilishning kompleks yondashuvi zamonaviy xavfsizlik talablarini ta'minlashi mumkin.

Integratsiyalashgan yondashuv himoya qilishning barcha usullari va vositalarini kompleks ishlab chiqishni nazarda tutadi.

Kompyuter tarmoqlarida axborot xavfsizligini ta'minlashning asosiy usullari va vositalarini qisqacha ko'rib chiqamiz.

Axborot xavfsizligi usullari quyidagilarga bo'linadi:

· to'siqlar
· kirish nazorati
· niqoblash
· tartibga solish
· majburlash
· motivatsiya

To'siq - tajovuzkorning himoyalangan ma'lumotlarga (kompyuter, tarmoq uskunalari) yo'lini jismoniy blokirovka qilish usuli

Kirish nazorati - bu barcha tizim resurslaridan foydalanishni tartibga solish orqali axborotni himoya qilish usuli. Kirish nazorati quyidagi xavfsizlik xususiyatlarini o'z ichiga oladi:

- har bir ob'ektga shaxsiy identifikatorni belgilash orqali tizim foydalanuvchilari, xodimlari va resurslarini identifikatsiyalash;
- ob'ekt yoki predmetni ularga taqdim etilgan identifikator orqali aniqlash;
- so'ralgan resurslar uchun ruxsatnomalarni tekshirish;
- himoyalangan resurslarga qo'ng'iroqlarni ro'yxatga olish;
- ruxsatsiz harakatlarga urinishlarga javob

Maskalash - ma'lumotni kriptografik yopish (shifrlash) orqali himoya qilish usuli. Hozirgi vaqtda bu usul eng ishonchli hisoblanadi.

Uchta asosiy algoritm ma'lum: DES algoritmi, zamonaviy Clipper (Capston) algoritmi va ommaviy tashabbus deb ataladigan algoritm - PGP algoritmi.

DES (Data Encryption Standard) shifrlash algoritmi 1970-yillarning boshida ishlab chiqilgan. Shifrlash algoritmi kalit uzunligi 64 ta belgidan iborat bo'lgan integral sxema sifatida amalga oshirildi (56 belgi to'g'ridan-to'g'ri shifrlash algoritmi uchun va 8 tasi xatolarni aniqlash uchun ishlatiladi).

O'sha paytdagi algoritmlarni hisoblash shifrlash kaliti 72 kvadrillion kombinatsiyaga ega bo'lishi mumkinligini ko'rsatdi. DES algoritmi AQSHda 1977-yilda axborotni qayta ishlashning federal standarti sifatida qabul qilingan va 80-yillarning o‘rtalarida u xalqaro standart sifatida tasdiqlangan bo‘lib, har besh yilda bir marta tasdiqlash protsedurasidan o‘tadi. Axborotni himoya qilish darajasini baholash uchun tahlilchilar quyidagi faktni keltiradilar: 1 million dollarlik zamonaviy kompyuter shifrni 7 soatda, 10 million dollarga – 20 daqiqada, 100 million dollarga – 2 daqiqada ochib beradi. AQSh Milliy xavfsizlik agentligida shunday kompyuter mavjud.

Axborotni shifrlashning yangi usuli - Clipper texnologiyasi AQSh Milliy Xavfsizlik Agentligi tomonidan telefonlarni eshitishdan himoya qilish uchun ishlab chiqilgan.

Ma'lumotlarni himoya qilish uchun bu usul Capston deb ataladi. Usul ikkita kalit - sekundiga 1 gigabitgacha bo'lgan tezlikda ma'lumotlarni shifrlashni ta'minlaydigan mikrochiplar printsipiga asoslanadi. Foydalanuvchilar kalitlarni davlat idoralari yoki xususiy kompaniyalar tomonidan boshqariladigan ikkita nuqtada olishadi. Kalit tizimi ikkita integral mikrosxemalar "Clipper chip" va "Capston chip" va SKIPJACK shifrlash algoritmidan iborat. Shifrlash algoritmi 32 ta o'tishda 80 belgili kalit yordamida ma'lumotlarning belgilar bloklarini shifrlaydi. Bu DES algoritmidan 16 million marta kuchliroq va faqat bir necha o'n yilliklar ichida 100 million dollarlik kompyuterlar shifrni ochishga qodir bo'ladi, deb ishoniladi.

2 daqiqada ma'lumot. Internet uchun SKIP (Internet Protocol uchun oddiy kalitlarni boshqarish) maxsus shifrlash protokoli ishlab chiqilgan bo'lib, u axborot oqimlarining shifrlanishini nazorat qiladi.

Shuni ta'kidlash kerakki, hozirgi vaqtda AQSh federal organlari SKIP protokolini eksport qilishni taqiqlaydi, shuning uchun ko'plab mamlakatlarda uning analogini yaratishga urinishlar qilinmoqda.

PGP (Pretty Good Privacy) kriptografik dasturi 1991 yilda amerikalik dasturchi F. Zimmermann tomonidan elektron pochta xabarlarini shifrlash uchun ishlab chiqilgan. PGP Internetga kirish uchun bepul va har qanday kompyuterga o'rnatilishi mumkin. PGP dasturining ishlash printsipi ikkita asosiy dasturdan foydalanishga asoslangan: biri jo'natuvchi uchun, ikkinchisi esa qabul qiluvchi uchun. Kalit dasturlar parollar bilan emas, balki parol bilan himoyalangan. Xabarni faqat ikkita kalit

yordamida hal qilish mumkin. PGP dasturi murakkab matematik algoritmdan foydalanadi, bu ikkita kalitdan foydalanish printsipi bilan birgalikda shifrni ochishni deyarli imkonsiz qiladi. PGP dasturlarining paydo bo'lishi AQSh huquqni muhofaza qilish doiralarida janjal keltirib chiqardi, chunki ular ma'lumotni nazorat qilish qobiliyatidan mahrum.

E'tibor bering, kriptografik algoritmlar elektron raqamli imzolarni himoya qilish uchun keng qo'llaniladi.

Kriptografik usullar haqida ko'proq ma'lumot olish uchun www.cripto.com yoki www.confident.ru saytiga tashrif buyuring

Tartibga solish - bu himoyalangan ma'lumotlarni avtomatlashtirilgan qayta ishlash, saqlash va uzatish uchun shunday shart-sharoitlarni yaratadigan axborotni himoya qilish usuli bo'lib, unga ko'ra ruxsat etilmagan ma'lumotlarni saqlash imkoniyati mavjud.

unga kirish imkoni minimal darajaga tushiriladi.

Majburlash - bu ma'lumotlarni himoya qilish usuli bo'lib, unda foydalanuvchilar va tarmoq ma'murlari himoyalangan ma'lumotlarni qayta ishlash, uzatish va ulardan foydalanish qoidalariga rioya qilishga majbur bo'ladilar.

moddiy, ma'muriy yoki jinoiy javobgarlik tahdidi.

Motivatsiya - foydalanuvchilarni va tarmoq ma'murlarini belgilangan axloqiy va axloqiy me'yorlarni buzmaslikka undaydigan himoya usuli.

Axborot xavfsizligi vositalari quyidagilarga bo'linadi:

· texnik vositalar
· dasturiy ta'minot
· tashkiliy vositalar
· axloqiy va axloqiy
· qonun chiqaruvchi.

Kriptografiya nima?

Kriptografiya – bu ma'lumotlarni kodlash orqali ularga ruxsatsiz kirishni cheklash texnologiyasi. Ushbu usulda ma'lumotlar maxsus algoritmlar yordamida shifrlanadi va faqat ruxsat berilgan tomonlar tomonidan maxsus kalitlar yordamida ochilishi mumkin. Kriptografiya orqali ma'lumotlarni shifrlash ularning tarmoq orqali osonlikcha o‘g‘irlanishi yoki buzilishining oldini oladi.

Kriptografik himoya turlari

Lokal kompyuter tarmoqlarida axborotlarni himoya qilish uchun kriptografiyaning bir necha asosiy usullari mavjud:

1.Simmetrik kalitli shifrlash

Simmetrik kriptografiyada ma'lumotlarni shifrlash va ochish uchun bitta kalit ishlatiladi. Bu usulda barcha tomonlar o‘zaro ma'lumot almashishdan oldin umumiy kalitga ega bo‘lishlari kerak. Bu usul tez ishlaydi, lekin kalitni xavfsiz tarqatish masalasi katta xavf tug‘dirishi mumkin.

2.Assimetrik kalitli shifrlash

Assimetrik kriptografiyada ikki xil kalit – ochiq kalit va yopiq kalit ishlatiladi. Ma'lumotlar ochiq kalit bilan shifrlanadi va faqat yopiq kalit bilan ochilishi mumkin. Bu usulning afzalligi kalitlarni tarqatishdagi xavfsizlik masalalarini bartaraf etishidir, chunki faqat ochiq kalit hammaga beriladi, yopiq kalit esa sir saqlanadi.

3.Gibrid shifrlash

Gibrid shifrlashda simmetrik va assimetrik kriptografiya birgalikda qo‘llaniladi. Bu usulda ma'lumotlar simmetrik kalit bilan shifrlanadi, ammo simmetrik kalit assimetrik kalitlar yordamida uzatiladi. Gibrid usul yuqori tezlik va xavfsizlikni ta’minlaydi.

Lokal kompyuter tarmoqlarida kriptografik himoya qilish afzalliklari

1.Maxfiylikni ta'minlash

Ma'lumotlarni kriptografik himoya qilish orqali faqat ruxsat berilgan foydalanuvchilar ma'lumotlardan foydalanishi mumkin bo‘ladi. Bu esa tarmoq orqali o‘tgan ma'lumotlar buzilishi yoki o‘g‘irlanishi xavfini kamaytiradi.

2.Ma'lumot yaxlitligini himoya qilish

Ma'lumotlar kriptografik himoya yordamida buzilish yoki o‘zgartirishdan himoyalanadi. Foydalanuvchilar ma'lumotni qabul qilganda, uning asl holatda ekanligini tekshira olishadi.

3.Tasdiqlash va autentifikatsiya

Kriptografik texnologiyalar orqali foydalanuvchilar va tizimlar o‘zaro autentifikatsiyadan o‘tadi. Bu esa tarmoqda ruxsatsiz kirishni oldini oladi.

Kriptografik himoya qilishning qo‘llanilishi

Lokal kompyuter tarmoqlarida kriptografiya turli sohalarda qo‘llaniladi:

•Tashkilotlararo ma'lumot almashish

Tashkilotlar o‘rtasida tarmoq orqali uzatiladigan ma'lumotlar kriptografik himoya qilinishi kerak. Bu, ayniqsa, moliyaviy va shaxsiy ma'lumotlar bilan ishlaydigan tashkilotlar uchun juda muhim.

•Ichki tarmoq xavfsizligi

Kompaniyaning ichki tarmog‘ida ishchilar orasida uzatiladigan ma'lumotlar shifrlangan bo‘lsa, tarmoqda har qanday ichki va tashqi hujumlarning oldi olinadi.

•VPN (Virtual Privat Network)

VPN texnologiyasi kriptografiyani qo‘llaydi va foydalanuvchilarga xavfsiz tarmoq orqali ma'lumotlar almashish imkoniyatini beradi. Bu usul tashqi tarmoqlar orqali kiruvchi foydalanuvchilar uchun muhimdir.

Foydalanilgan adabiyotlar:

1. Yo’ldoshev Shohruhbek Zokirjon o’g’li TA'LIMDA AXBOROT XAVFSIZLIGINING HOZIRGI HOLATI// TA’LIM JARAYONIDA RAQAMLI TEXNOLOGIYALARNI JORIY ETISH SAMARADORLIGI mavzusidagi Respublika ilmiy-amaliy, 2023. 94-96 b.
2. Yo‘ldoshev Sh.Z. Ta'limda axborot xavfsizligining hozirgi holati//Ta’lim jarayonida raqamli texnologiyalarni joriy etish samaradorligi mavzusidagi Respublika ilmiy-amaliy konferensiyasi, 2023. 94-96 b.
3. Sh.Z.Yo‘ldoshev tarmoq xavfsizligi dasturlari va vositalari turlari//Hayot davomida ta’lim paradigmasi diskursida andragogikaning kompetensiyaviy imkoniyatlari xalqaro ilmiy-amaliy konferensiya, 2024. 544-548 b.
4. Sh.Z.Yo‘ldoshev IoT tarmoqlarining turlari, ularning umumiy ko‘rinish va foydalanish holatlari// UzMU xabarlari, 2024. 108-110 b.
5. Xurramov, A., & Xushboqova, O. (2024). Bulutli texnologiyalarda tahdidlar va himoya. Молодые ученые, 2(24), 93–94

.