

AXBOROT XAVFSIZLIGINI TA'MINLASHNING ASOSIY VAZIFALARI VA DARAJALARI

Sodiqova Shahloxon Sherzodjon qizi

TerDU Matematika va informatika yo'nalishi talabasi

Xurramova Muharrama Xolboy qizi

TerDU Matematika va informatika yo'nalishi talabasi

<https://doi.org/10.5281/zenodo.7312609>

Annotatsiya. Jamiyatning jadal sur'atlarda axborotlashtirilishi sababli axborot xavfsizligi muammosi nihoyatda dolzarb va doimo shunday bo'lib qoladi. Ushbu maqolada axborot xavfsizligi tushunchasi va uning vazifalari, axborot xavfsizligiga bo'ladigan tahdidlar, kriptologiya maqsadlari va uning qarama-qarshi ikki yo'nalishi ya'ni kriptografiya va kriptotahlil yo'nalishlari haqida batafsil ma'lumotlar berilib o'tilgan. Axborotlarni ishonchli himoyalash masalalari ko'rib o'tildi.

Kalit so'zlar: Axborot xavfsizligi, konfidensiallik, yaxlitlik, indentifikatsiya, autentifikatsiya, vakolat berish, foydalanishni nozoratlash, mulklik huquqi, sertifikatatsiya, imzo, voz kechmaslik, sanasini yozish, olganligiga tilxat berish, bekor qilish, anonimlik.

ОСНОВНЫЕ ЗАДАЧИ И УРОВНИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. В связи с быстрым информированием общества проблема информационной безопасности является чрезвычайно актуальной и всегда будет оставаться таковой. В данной статье представлена подробная информация о понятии информационной безопасности и ее задачах, угрозах информационной безопасности, целях криптологии и двух ее противоположных направлениях, а именно криптографии и криптоанализе. Рассмотрены вопросы надежной защиты информации.

Ключевые слова: информационная безопасность, конфиденциальность, целостность, идентификация, аутентификация, авторизация, контроль использования, право собственности, сертификация, подпись, неотказуемость, дата, получение, отзыв, анонимность.

MAIN TASKS AND LEVELS OF ENSURING INFORMATION SECURITY

Abstract. Due to the rapid information of the society, the problem of information security is extremely urgent and will always remain so. This article provides detailed information about the concept of information security and its tasks, threats to information security, the goals of cryptology and its two opposing directions, namely, cryptography and cryptanalysis. Issues of reliable protection of information were considered.

Keywords: Information security, confidentiality, integrity, identification, authentication, authorization, control of use, ownership, certification, signature, non-repudiation, date, receipt, revocation, anonymity.

KIRISH

Kompyuter texnikasi va axborot tizimlarining iqtisodda, boshqarishda, aloqada, ilmiy tadqiqotlarda, ta'limda, xizmat ko'rsatish sohasida, tijoratda, moliya va inson faoliyatining boshqa sohalarida qo'llashining rivoji axborotlashtirish va umuman, jamiyat rivojini belgilovchi yo'nalish hisoblanadi. Kompyuter texnikasining qo'llanilishi evaziga erishuvchi samara axborot ishlanishi ko'lamining oshishi bilan ortib boradi. Ushbu texnikaning qo'llanish sohalari va

ko'lamini uning ishlashining ishonchliligi va barqarorligi muomalari bilan bir qatorda unda aylanuvchi axborot xavfsizligini ta'minlash muammosini tug'diradi.

Axborotni muhofaza qilish masalalari bilan kriptologiya (kruptos-maxiy, logos-ilm) fani shug'ullanadi. Kriptologiya maqsadlari o'zaro qarama-qarshi ikkita yo'nalishiga ega bo'lgan-kriptografiya va kriptotahlil yo'nalishlariga ajraladi.

TADQIQOT MATERIALLARI VA METODOLOGIYASI

Kriptografiyaning ochiq ma'lumotlarni shifrlash masalalarining matematik uslublari bilan shug'ullanishi to'g'risida yuqorida aytib o'tildi.

Kriptotahlil esa shifrlash uslubi (kaliti yoki algoritmi) ni bilmagan holda shifrlangan ma'lumotni asl holatini (mos keluvchi ochiq ma'lumotni) topish masalalarini yechish bilan shug'ullanadi.

Hozirgi zamon kriptografiyasi quyidagi bo'limlarni o'z ichiga oladi:

- Simmetrik kriptotizimlar.
- Ochiq uslubga yoki yana boshqacha aytganda ochiq kalitlar algoritimiga asoslangan kriptotizimlar.
- Eliktron raqamli imzo kriptografik tizimlari.
- Kriptotizimlar uchun kriptobardoshlik kalitlarini ishlab chiqish va ulardan foydalanishni boshqarish.

Tadqiqot materiallari va metodologiyasi.

TADQIQOT NATIJALARI

Axborot xavsizligini ta'minlash muntazam va kompleks xarakterga ega ko'p qirrali faoliyatni amalga oshirishni ko'zda tutadi. Uni amalga oshirishda axborot xavsizligidan manfaatdor taraflar oldida qo'yiladigan vazifalarga alohida e'tibor berish zarur. Ushbu turli-tuman vazifalarni bir necha quyidagi asosiy guruhlariga ajratish mumkin:

1. Axborotdan foydalanishni ta'minlash, ya'ni maqbul vaqt mobaynida axborot xizmatini olish hamda axborotni olishda ruhsatsiz taqiqlanishni bartaraf etish;
2. Axborot yaxlitligini ta'minlash, ya'ni axborotning ruhsatsiz modifikatsiyalanishini yoki buzilishini bartaraf etish;
3. Axborot konfidensialligini ta'minlash, ya'ni axborotdan ruhsatsiz tanishishni bartaraf etish.

Axborot xavsizligi – mamlakat madaniy mulkining, xo'jalik sub'ektlari va fuqorolar intellektual mulkining, davlat va kasbiy sirga maxsus ma'lumotlarning ishonchli himoyalanganligi holati.

Odatda, bir-biridan axborot xavsizligining huquqiy, texnik, moliyaviy, tashkiliy va boshqa resursli ta'minot bilan farqlanuvchi axborot xavsizligi sub'ektlarining quyidagi to'rtta kategoriyasi ajratiladi:

- butun bir davlat;
- davlat tashkilotlari;
- tijorat tuzilmalari;
- alohida fuqoralar.

MUHOKAMA

Yuqorida keltirilgan axborot xavsizligini ta'minlashdagi asosiy vazifalar qamrab olgan quyidagi keng spektrli masalalarni ko'rib chiqish joiz hisoblanadi:

- konfidensiallik;
- yaxlitlik;
- indentifikatsiya;
- autentifikatsiya;
- vakolat berish;
- foydalanishni nozoratlash;
- mulklik huquqi;
- sertifikatatsiya;
- imzo;
- voz kechmaslik;
- sanasini yozish;
- olganligiga tilxat berish;
- bekor qilish;
- anonimlik.

Yuqorida keltirilgan vazifalar mavjud axborot dunyosi ehtiyojiga asosan tavsiflangan. Vaqt o'tishi bilan ba'zi vazifalar o'z dolzarbligini yo'qotishi va aksincha, yechimini kutuvchi yangi vazifalar paydo bo'lishi mumkin.

XULOSA

Xulosa qilib shuni aytish mumkinki, axborotlarni saqlash va uzatish tizimlari bir tomondan takomillashib murakkablashgan va ikkinchi tomondan axborotlardan foydalanuvchilar uchun keng qulayliklar vujudga kelgan davrda, axborotlarni maqsadli boshqarishning qator muhim masalalari kelib chiqadi. Bunday masalalar qatoriga katta hajimdagi axborotlarning tez va sifatli uzatish hamda qabul qilish axborotlarni ishonchliligini ta'minlash, axborotlar tizimida axborotlarni begona shaxslardan (keng ma'noda) muhofaza qilish kabi ko'plab boshqa masalalar kiradi.

REFERENCES

1. S. K. Ganiyev, M. M. Karimov, K.A. Tashev. Axborot xavfsizligi. T. , 2017 yil.
2. S. S. Qosimov. Axborot xavfsizligini ta'minlashning kriptografik usullari va ularning qo'llanilishi.
3. M. Aripov, B. Begalov, U. Begimqulov, M. Mamarajabov. Axborot texnologiyalari. T. 2009 yil.