

AXBOROT XAVFSIZLIGINI TA'MINLASH HAMDA AXBOROT SOHASIDA MILLIY XAVFSIZLIK CHORALARINI KO'RISH

Narsafarova Ra'no Meganovna

Annotatsiya. Jamiyatning ommaviy axborotlashtirilishi sababli axborot xavfsizligi muammosi nihoyatda muhim hamda doimo shunday bo'lib qoladi. Mazkur maqolada axborot xavsizligi 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 chuqur informatsiyalar keltirib o'tilgan. Axborotlarni ishonchli himoyalash masalalari o'rganildi.

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

ОСНОВНЫЕ ЗАДАЧИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, А ТАКЖЕ ПРИНЯТИЯ МЕР НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ В ОБЛАСТИ ИНФОРМАЦИИ

Абстрактный. Проблема информационной безопасности чрезвычайно важна и всегда будет оставаться таковой в связи с массовой информатизацией общества. В данной статье представлена подробная информация о понятии информационной безопасности и ее задачах, угрозах информационной безопасности, целях криптологии и двух ее противоположных направлениях, т. е. криптографии и криптоанализе. Изучены вопросы надежной защиты информации.

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

PRINCIPAL TASKS OF ENSURING INFORMATION SECURITY AS WELL AS TAKING NATIONAL SECURITY MEASURES IN THE FIELD OF INFORMATION

Abstract. The problem of information security is extremely important and will always remain so due to the mass information of society. This article provides in-depth information about the concept of information security and its tasks, threats to information security, the goals of cryptology and its two opposing directions, i.e., cryptography and cryptanalysis. Issues of reliable protection of information were

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

KIRISH

Bugun hayotimizning barcha jabhalariga axborot-kommunikatsiya va kompyuter texnologiyalarining kirib kelganligi ayni haqiqat. Bu o'zgarishlarning asosini axborotlashtirish, telekommunikatsiya va kompyuter texnologiyalari tashkil etadi. XXI asr - axborotlashgan jamiyat asridir. "Axborot ijtimoiy-iqtisodiy, madaniy taraqqiyotning muhim omilidir. Shu sababli ham u inson tafakkuriga turli yo'nalishlarda ta'sir etuvchi, insoniyatning hayoti va taqdirini u yoki bu tomonga burib yuboruvchi, goh ijobiy, goh salbiy mohiyat kasb etuvchi qudratli vositaga aylandi"

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 sohaları vako'lami 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.
- Elektron raqamli imzo kriptografik tizimlari.

- Kriptotizimlar uchun kriptobardoshlik kalitlarini ishlab chiqish va ulardan foydalanishni boshqarish.

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 quydagi 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 xavfsizligi - deganda tabiiy yoki sun'iy xarakterdagi tasodifiy yoki qasddan qilingan ta'sirlardan axborot va uni qo'llab-quvvatlab turuvchi infrastukturaning himoyalanganligi tushuniladi. Bunday ta'sirlar axborot sohasidagi munosabatlarga, jumladan, axborot egalariga, axborotdan foydalanuvchilarga va axborotni muhofaza qilishni qo'llab quvvatlovchi infrastrukturaga jiddiy zarar yetkazishi mumkin. Axborot xavfsizligini ta'minlashga yo'naltirilgan himoya harakatlari qator kattaliklar bilan tavsiflanishi mumkin: tahdid xarakteri, harakat usullari, uning tarqalganligi, o'rab olish mashtabi kabilar. O'zbekiston Respublikasining 2002-yil 12-dekabrda №439-II-sonli "Axborot erkinligi prinsiplari va kafolatlari to'g'risida"gi qonunida axborot xavfsizligi axborot borasidagi xavfsizlik deb belgilangan va u axborot sohasida shaxs, jamiyat va davlat manfaatlarining himoyalanganlik holatini anglatadi.

Axborot xavfsizligi – 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.

МУХОКАМА

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;
- sertifikatziya;
- 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.

Hozirgi shiddat bilan rivojlanib borayotgan darda biz insonlarnin hech birimiz kundalik turmush tarzimizni axborot va axborot ulashuvchi vositalarisiz tasavvur qila olmaimiz. Ushbu axborot olish jarayonida biz internet, ijtimoiy tarmoqlar, tilvidinya, gazeta-jurnallar, kitoblardan keng foydalanamiz. Ko'pincha biz ushbu olayotgan axborotlarimizning haqqiqiymi, aniqmi, haqiqatga mosmi, mualifi kim, qaysi tashkilot yoki nashrning axboroti ekanligiga va qanday turdagi axborot ekanligiga qiziqmaymiz. Bu esa bizning axborot olish madaniyatiga ega emasligimizni va kata xatolarga yo'l

qo'yishimizga olib kelishini hech birimiz o'ylab ko'rmaymiz. Vaholanki axborotni qanday yo'qotish mumkinligini va bu qanday oqibatlarga olib kelishini barcha ham tushunavermaydi. "Aytishingiz mumkin qanday yo'qotish yoki oqibat!" deb. Hozir sizga axborot sohasidagi jahonda ro'y bergan ba'zi voqealarni misol keltiraman. Misol uchun Xakerlar hujumi oqibatida 150 mamlakatda 200 ming kishi va ko'plab tashkilotlar zarar ko'rdi. Bu haqda Yevropa politsiya agentligi (Yevropol) rahbari Rob Ueynrayt ma'lumot berdi, deb xabar qiladi "RBK".

Axborotni muhofaza qilish tizimlaridan foydalanish amaliyoti shuni ko'rsatmoqdaki, faqatgina kompleks axborotni muhofaza qilish tizimlari samarali bo'lishi mumkin. Unga quyidagi chora-tadbirlar kiradi:

1. Qonunchilik-axborot himoyasi sohasida yuridik va jismoniy shaxslarning, shuningdek davlatning huquq va majburiyatlarini qat'iy belgilovchi qonuniy aktlardan foydalanish.

2. Ma'naviy-etik-obyektda qat'iy belgilangan o'zini tutish qoidalarining buzilishi ko'pchilik xodimlar tomonidan keskin salbiy baholanishi joriy etilgan muhitni hosil qilish va qo'llab quvvatlash.

3. Fizik-himoyalangan axborotga begona shaxslarning kirishini taqiqlovchi fizik to'siqlar yaratish.

4. Ma'muriy-tegishli maxfiylik rejimi, kirish va ichki rejimlarni tashkil etish.

5. Texnik-axborotni muhofaza qilish uchun elektron va boshqa uskunalardan foydalanish.

6. Kriptografik-ishlov berilayotgan va uzatilayotgan axborotlarga noqonuniy kirishni oldini oluvchi shifrlash va kodlashni tatbiq etish.

7. Dasturiy-foydalana olishlilikni chegaralash uchun dastur vositalarini qo'llash. Fizik, apparatli, dasturli va hujjatli vositalarni o'z ichiga oluvchi barcha axborot tashuvchilarga kompleks holda himoya obyekti sifatida qaraladi.

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. Milliy axborot

resurslari xar bir davlatning iqtisodiy va harbiy salohiyatini tashkil qiluvchi omillaridan biri bo'lib xizmat kilmokda. Ushbu resursdan samarali foydalanish mamlakat xavfsizligini va demokratik axborotlashgan jamiyatni muvaffaqiyatli shakllantirishni ta'minlaydi. Bunday jamiyatda axborot almashuvi tezligi yuksaladi, axborotlarni yig'ish, saqlash, qayta ishlash va ulardan foydalanish bo'yicha ilg'or axborot – kommunikatsiyalar texnologiyalarini qo'llash kengayadi. Turli xildagi axborotlar xududiy joylashishidan qat'iy nazar bizning kundalik hayotimizga Internet halqaro kompyuter tarmog'i 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 axborotlarning tarqalishi mexanizmini boshqara olmay qolmoqda.

FOYDALANILGAN ADABIYOTLAR (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.
4. O'zbekiston Milliy ensiklopediyasi. -T.: Davlat ilmiy nashiryoti, 2000.
5. Гаффарова Г. Ахборот ва ахборотлаштириш жараёнларининг фалсафий-методологик муаммолари. Фалс. фан. номз. ...дис. –Тошкент, 2008.