SHAXSIY KOMPYUTERDA DISKLARNI VA FAYLLARNI SHIFRLASH

Nurmatova Azimaxon Abdullajon qizi
Farg‘ona ICHSHUI kasb-hunar maktabi Informatika va axborot texnologiyalari fani o‘qituvchisi

Annotatsiya: *SHaxsiy kompyuterda disklarni va fayllarni shifrlash xaqida ma’lumotlar berilgan.*

Kalit so‘zlar: *shaxsiy kompyuter, , zamonaviy bilim, informatika va axborot texnologiyalar, shifrlash, disklarni shifrlash, fayllarni shifrlash. kriptografik algoritm.*

Bugungi kunda axborot jamiyatini rivojlantirishning zaruriy sharti bu kiberxavfsizlikdir, uni xavfsizlikning texnik va qonunchilikgacha bo‘lgan deyarli cheksiz ro‘yxati va ularni hal qilish yo‘li bilan ta’minlash mumkin.

Zamonaviy sharoitda, kiberxavfsizlik masalalari alohida kompyuter vositasida axborot xavfsizligi darajasidan har bir davlatning axborot va milliy xavfsizligining ajralmas qismi sifatida yagona kiberhavfsizlik tizimini yaratish darajasigacha boradi.

Raqamli qurilma (kompyuter, smartfon yoki tashqi saqlash qurilmasi) tomonidan qayta ishlanuvchi yoki unda saqlanuvchi barcha ma’lumotlar mohiyatdan olganda nol va birlarning turli ketma-ketligidan, ya’ni ikkilik tizimidagi koddan iborat. Barcha kompyuterlar va smartfonlar ushbu formatda ishlaganligi sababli, raqamli ma’lumotlar har qanday shunga o’xshash qurilmada yaratilishi, qayta ishlanishi va saqlanishi mumkin.

Shifrlash ikkilik ma’lumotlarni murakkab kodga aylantiradi, uni faqat maxfiy kalitga (shifrni ochish kaliti deb nomlanadi) ega yoki parolni bilgan odamlargina o’qiy oladi. Begonalar shifrlangan ma’lumotlarga kirish huquqini qo’lga kiritganda ham, ular kodni ochib ham, o’zgartib ham olmaydi.

Axborotni kriptografik himoyasi, hususan, shifrlash algoritmlari amalda keng qo‘llaniladi. Masalan, saqlash qurilmalarida ma’lumotlarni shifrlash yoki tarmoq bo‘ylab uzatiladigan axborotni shifrlab uzatishni misol tarzda keltirish mumkin.

Umuman olganda ma’lumotni shifrlashda ma’lum algoritmdan foydalaniladi. Ushbu algoritm biror bir operasion tizim uchun (masalan, Windows OT, Linux OT, Android OT) mo‘ljallangan dastur ko‘rinishida yoki maxsus qurilma ko‘rinishida (masalan, maxsus prosessorlar, USB token, smart karta va h.) bo‘lishi mumkin.

Kriptografik algoritmlar amalda quyidagi ko‘rinishdagi vositalar sifatida qo‘llaniladi :

- apparat ko‘rinishdagi vositalar;
- apparat-dasturiy ko‘rinishdagi vositalar;
- dasturiy ko‘rinishdagi vositalar.

Apparat-dasturiy shifrlash – shifrlash jarayoni bo‘lib, buning uchun maxsus ishlab chiqilgan hisoblash qurilmasidan foydalaniladi. Unga misol tariqasida,

ruToken USB shifrator qurilmasini ko‘rsatish mumkin (1 - rasm).

1-rasm ruToken USB shifrator qurilmasi – Rossiya Federasiyasida ishlab chiqariluvchi qurilma bo‘lib, undan asosan Rossiya Federasiyasining kriptografik algoritmlarida amalga oshirilgan. Masalan, ishlab chiqarilgan Rutoken S qurilmasining umumiy xarakteristikalari quyidagicha :

- shifrlash kalitlari, ERI kalitlari va turli sertifikatlarni xavfsiz saqlash uchun foydalaniladi;
- ushbu tokendan foydalanish uchun PIN kodni kiritish talab etiladi;
- diskdagi ma’lumotlarni shifrlash uchun qo‘llaniladi;
- tokenda mehmon, foydalanuvchi va ma’mur darajalari mavjud;
- Microsoft Windows 10/8.1/2012R2/8/2012/7/2008R2/ Vista/2008/XP/2003, GNU/Linux, Apple macOS/OSX muhitlarida foydalanish mumkin;
- 32, 64 va 128 KB xotiraga ega EEPROM;
- USB 1.1 va undan yuqori interfeysga ega;
- 58x16x8mm (mikro-token 17,8x15,4x5,8mm) o‘lchamga ega;
- 6,3g (mikro-token 1,6g) og’irlikka ega.

Apparat shifrlash o‘ziga xos quyidagi xususiyatlarga ega :

- saqlagichda (qurilmada) joylashgan maxsus prosessordan foydalaniladi;
- prosessorda shifrlash kalitini generasiyalash uchun maxsus kalit generatori mavjud bo‘lib, foydalanuvchi kiritgan parol asosida qulfdan yechiladi;
- asosiy tizimni (qurilma ulangan tizim, masalan, kompyuterdagi) shifrlash uchun foydalanmaslik orqali, samaradorlikka erishiladi;
- asosiy tizimni (qurilma ulangan tizim, masalan, kompyuterdagi) shifrlash uchun foydalanmaslik orqali, samaradorlikka erishiladi;
- kalitlar va boshqa maxfiy kattaliklar apparatda shifrlash orqali himoyalangan;
- autentifikasiya apparat-qurilmaga nisbatan amalga oshiriladi;
- o‘rta va katta hajmdagi tashkilotlar sharoitida yuqori iqtisodiy samaradorlik beradi va madadlashning oddiyligi;
- qurilmada amalga oshiriluvchi doimiy mavjud shifrlash funksiyasi;
- qo‘shimcha drayver yoki dasturlarni o‘rnatishning zaruriyati yo‘q;

- ma’lumotlar keng tarqalgan hujum usullaridan, parolni to‘liq tanlash usuli, zararli dasturni kiritish asosidagi hujumlar va kalitni topishga qaratilgan hujumlardan himoyalangan;
- amalga oshirish, dasturiy vositaga qaraganda, yuqori narx talab etadi.

Dasturiy shifrlash kompyuter vositasi yordamida disklarni, fayllarni, kataloglarni va turli ma’lumot saqlash vositalaridagi axborotni shifrlash va deshifrlash jarayonini amalga oshiradi. Umumiy holda dasturiy shifrlash vositalarini quyidagi guruhlarga ajratish mumkin:

- diskni shifrlash dasturiy vositalari (Disk encryption software);
- fayl/ katalogni shifrlash dasturiy vositalari (File/folder encryption);
- ma’lumotlar bazasini shifrlash dasturiy vositalari (Database encryption);
- aloqani shifrlash dasturiy vositalari (Communication encryption software).

2-rasmda diskni shifrlashda foydalaniluvchi TrueCrypt dasturiy vositasining ko‘rinishi keltirilgan.

2-rasm. TrueCrypt dasturiy vositasi

Ushbu dasturlash vositasi quyidagi xususiyatlarga ega:

- C, C++, Assembly dasturlash tillaridan foydalanib yozilgan;
- Windows, macOS va Linux OTlarida foydalanish mumkin;
- 3.30 MB hajmga ega;
- ushbu dasturiy vositada AES, Serpent va Twofish blokli shifrlash algoritmlaridan foydalaniladi.

Dasturiy shifrlash o‘ziga xos bo‘lgan quyidagi xususiyatlarga ega :

- shifrlash uchun boshqa dasturlar bilan bir vaqtning o‘zida kompyuter resursidan foydalanadi;
- kompyuterning himoyalanganlik darajasi saqlagichning himoyalanganlik darajasini belgilaydi;
- foydalanuvchi tomonidan kiritilgan paroldan ma’lumotni shifrlash kaliti sifatida foydalaniladi;
- dasturni yangilab turish talab etilishi mumkin;

- katta bo‘lmagan tashkilotlar uchun foydalanish yuqori iqtisodiy samaradorlik beradi;
- ixtiyoriy ma’lumotni saqlash usullari uchun shifrlashni amalga oshirish imkoniyati mavjud;
- parolni to‘liq tanlash hujumiga yoki parolni topishga qaratilgan boshqa hujumlarga bardoshsiz;
- apparat shifrlashga qaraganda kam sarf xarajat talab etadi.

Fayllarni shifrlash uchun quyidagi dasturlar tavsiya etiladi:

1.VeraCrypt:

- Ochiq kodli, multiplatforma (Windows, macOS, Linux) shifrlab/deshifrlab dastur;
- Disk, ajratilgan hajmlar va konteynerlarni shifrlab saqlash imkonini beradi;
- AES, Twofish, Serpent kabi kuchli shifrlanish algoritmlarini qo‘llab-quvvatlaydi;
- Foydalanuvchi interfeysi va boy funksiyonalligi bilan ajralib turadi.

3.7-Zip:

- Bir nechta fayl formatlarini (ZIP, TAR, gz, bzip2 va h.k.) qo‘llab-quvvatlaydi;
- Fayllarni AES-256 algoritmi yordamida shifrlab saqlash imkoniyatiga ega;
- Keng tarqalgan va ommabop arxivlash dasturi.

3.GNU Privacy Guard (GPG/PGP):

- Ochiq kodli, keng tarqalgan maxfiylik va raqamli imzo uchun vosita;
- Fayllarni, shaxsiy kalitlar yordamida shifrlab saqlash va uzatish imkonini beradi;
- Elektron pochta xabarlarini maxfiy almashuv uchun ham qo‘llaniladi.

4.Cryptomator:

- Bulutda saqlangan fayllarni shifrlab saqlash uchun ilovasi;
- Zero-knowledge yondashuv asosida ishlaydi, ya'ni hech qanday ma'lumot serverda saqlanmaydi;
- Oddiy va qulay interfeysi bilan ajralib turadi.

5.BoxCryptor:

- Bulut xizmatlarida (Google Drive, Dropbox, OneDrive va boshqalar) saqlangan fayllarni shifrlay oladi;
- AES-256 algoritmi va 4096-bit RSA kalitlaridan foydalanadi;
- Keng tarqalgan va ishonchli shifrlab saqlash vositasi.

Ushbu dasturlar orasida VeraCrypt, 7-Zip va GPG/PGP ko‘proq tavsiya etiladi, chunki ular ochiq kodli, ko‘p funksiyali va keng tarqalgan. Shuningdek, Cryptomator va BoxCryptor ham bulutda saqlangan fayllarni shifrlab saqlash uchun yaxshi tanlovlar hisoblanadi.

Disklarni va fayllarni shifrlash uchun quyidagi usullardan foydalanish mumkin:

Disk Shifrlab (Full Disk Encryption - FDE):

Butun disk yuzasi bo‘yicha shifrlanadi;

- Operativ tizimni ishga tushirishda yoki diskni ulashda avtomatik ravishda shifrlanadi;
- Windows BitLocker, macOS FileVault, Linux Veracrypt/LUKS kabi vositalardan foydalanish mumkin.

Fayllar Shifrlab (File-level Encryption):

- Alohida fayllarni yoki papkalarni alohida shifrlab qo‘yish;
- Masalan, Windows Encrypted File System (EFS), VeraCrypt, 7-Zip, GPG kabi vositalardan foydalanish mumkin;
- Faqat zarur fayllar himoyalanganligi uchun .

Bulutli xizmatlar uchun shifrlab saqlash:

Bulutda saqlashda fayllarni shifrlashda maxsus shifrlab olish dasturlaridan foydalanish. Masalan, VeraCrypt, BoxCryptor, Cryptomator kabi vositalar

Taqsimlangan disklar (Encrypted Volumes):

Yuqori xavfsizlik talab qilinadigan fayllarni alohida shifrlangan hajmlarda saqlash

VeraCrypt, DiskCryptor, Linux LUKS kabi vositalar yordamida.

Yuqorida keltirilgan usullar orqali disklarni, fayllarni va ma’lumotlarni xavfsiz saqlash va uzatish mumkin. Ushbu usullarni qo‘llashda maxfiylik, yaxlitlik va muolajalar samaradorligini ta'minlash uchun qo‘shimcha parametrlarni sozlash, kalitlar saqlash va yetarli xavfsizlik choralari ko‘rish muhim.

FOYDALANILGAN ADABIYOTLAR VA INTERNET MANBALAR:

1. S.K. GANIYEV, A.A. GANIYEV, Z.T. XUDOYQULOV. Kiberxavfsizlik asoslari. O‘quv qo‘llanma. TOSHKENT 2020.

2. Abduqodirov A., Xaitov A., Rashidov R. Axborot texnologiyalari.- T.: «O‘qituvchi», 2002 y.

3. https://whatsappss.ru/uz/security/kak_zashifrovat_dannye_na_kompjutere.html

4. https://uz.eyewated.com/fayllarni-qanday-qilib-shifrlash-kerak-va-nima-uchun-kerak/

5. https://cyber-star.org/uz/cs-articles/why-you-should-encrypt-your-devices-uz/

6.https://kompy.info/9-maruza-disklarni-va-fayllarni-shifrlash-malumotlarni-xavfsiz.html

7. Горовик, А. А., & Турсунов, Х. Х. У. (2020). Применение средств визуальной разработки программ для обучения детей программированию на примере Scratch. Universum: технические науки, (8-1 (77)), 27-29.

8. Hamidullo o‘g‘li, T. H. (2024). RAQAMLI AXBOROTLARNI QAYTA ISHLASHDA BULUTLI TEXNOLOGIYALARDAN FOYDALANISHDA CLOUD-ANDROID, ICLOUD-APPLE IMKONIYATLARI VA FARQLARI. Scientific Impulse, 2(20), 189-193.

9. Hamidullo o‘g‘li, T. H. (2024). RAQAMLI TEXNOLOGIYADA UCH O‘LCHAMLI DASTURLARNING IMKONIYATALARI. Scientific Impulse, 2(21), 220-224.

10. Hamidullo o‘g‘li, T. H. (2024). ZAMONAVIY TA’LIMDA SMM SOHASINI XOZIRGI KUNDAGI O‘RNI. Scientific Impulse, 2(21), 215-219.

11. Zokirov, S. I., Sobirov, M. N., Tursunov, H. K., & Sobirov, M. M. (2019). Development of a hybrid model of a thermophotogenerator and an empirical analysis of the dependence of the efficiency of a photocell on temperature. Journal of Tashkent Institute of Railway Engineers, 15(3), 49-57.

12.Kamolovich, B. E., & Hamidullo o‘g‘li, T. H. (2024). RAQAMLI TEXNOLOGIYALARI DAVRIDA SOHA MUTAXASSISLIK FANI BO‘YICHA IQTIDORLI O‘QUVCHILAR BILAN ISHLASH. Scientific Impulse, 2(18), 125-131.

13.Тураев, А. А., Хайдаров, Р. М., & Хожиев, Ж. Ж. (2015). Фотовольтаический эффект в диодном режиме включения полевого транзистора. Молодой ученый, (23), 40-43.

14.Mamayusupovich, H. R. (2023). OPPORTUNITIES FOR THE DEVELOPMENT OF PROFESSIONAL COMPETENCE OF A TEACHER OF TECHNOLOGY. International Multidisciplinary Journal for Research & Development, 10(12).

15.Mamayusupovich, H. R. (2023). BO‘LAJAK TEXNOLOGIYA FANI O‘QITUVCHILARINI TAYYORLASH JARAYONIDA ELKTRON DARSLIKLARNI QO‘LLASHNING AHAMIYATI. Наука и технологии, 1(1).

16. Haydarov, R. (2022). TEXNOLOGIYA TA’LIMI O‘QITUVCHISINING TEXNOLOGIK MADANIYATI. Физико-технологического образование, (3).

17.Mamayusupovich, H. R. (2022). Design of Educational Technologies in the Development of Professional Competences of Technology Teachers.

18.Хайдаров, Р. М. (2021). ТЕХНОЛОГИЯ ТАЪЛИМИ ЎҚИТУВЧИСИНИНГ КАСБИЙ КОМПЕТЕНТЛИГИНИ ТАКОМИЛЛАШТИРИШ ТЕХНОЛОГИЯСИ. Образование и инновационные исследования международный научно-методический журнал, (1-Махсус сон), 273-277.

19.Hudaykulovna, M. F., & Qosimov, P. S. U. (2019). Formation of a Conscious Attitude to Study and Work, Ensuring Business Skills for Mental and Physical Development. European Journal of Research and Reflection in Educational Sciences Vol, 7(12).

20.Khudoikulovna, M. F. (2021). The role of heredity in the development of creativity. In Euro-Asia Conferences (Vol. 4, No. 1, pp. 5-6).

21.Khudoikulovna, M. F. (2021, March). THINKING MOTIVES THAT ENCOURAGE STUDENTS TO BE CREATIVE. In E-Conference Globe (pp. 65-66).

22.Мукумова, Ф. Х. (2021). МИЛЛИЙ ҲУНАРМАНДЧИЛИК ТАРИХИНИ ЎРГАНИШДА ЎҚУВЧИЛАРНИ ИЖОДКОРЛИККА ҚИЗИҚТИРИШНИНГ ДИДАКТИК ИМКОНИЯТЛАРИ: DOI: https://doi. org/10.53885/edinres. 2021.77. 73.052 Мукумова Феруза Худойқуловна Термиз давлат университети, технологик таълим кафедраси катта ўқитувчиси. Образование и инновационные

исследования международный научно-методический журнал, (1-Махсус сон), 154-159.

23.Мукумова, Ф. Х. (2021). ОСНОВНЫЕ КРИТЕРИИ ПОДГОТОВКИ УЧИТЕЛЯ К УЧЕБНОМУ ПРОЦЕССУ: DOI: https://doi. org/10.53885/edinres. 2021.83. 90.053 Мукумова Феруза Худайкуловна, Преподавательница Термезского государственного университета. Образование и инновационные исследования международный научно-методический журнал, (1-Махсус сон), 150-153.

24. Mamayusupovich, H. R. (2024). Development Of Professional Competence Of Future Teachers Of Technology In The Process Of Extracurricular Activities. Progress Annals: Journal of Progressive Research, 2(1), 35-37.

25. Кучаров, С. А. (2021). TEXNOLOGIYA TA'LIMI O'QITUVCHISINING TEXNOLOGIK MADANIYATI. Образование и инновационные исследования международный научно-методический журнал, (1-Махсус сон), 116-118.

26. Tursunov, H. H., & Hoshimov, U. S. (2022). TA'LIM TIZIMIDA KO'ZI OJIZ O'QUVCHILARNI INFORMATIKA VA AXBOROT TEXNOLOGIYALARI FANIDA O'QITISH TEXNOLOGIYALAR. Новости образования: исследование в XXI веке, 1(5), 990-993.

27. Hamidullo o'g'li, T. H. (2022). HOZIRGI KUNNING DOLZARB IMKONIYATLARI. JAWS VA NVDA DASTURLARI. Scientific Impulse, 1(2), 535-537.

28.https://winpcguide.ru/uz/configuring-wi-fi/what-does-the-system-disk-encryption-provide-create-an-encrypted-disk/