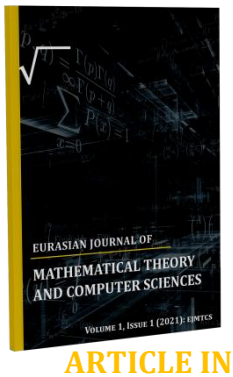
EURASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES
Innovative Academy Research Support Center
UIF = 8.3 | SJIF = 5.916 www.in-academy.uz



INFORMATIKA FANINI O‘QITISHDA AXBOROT XAVFSIZLIGI TUSHUNCHALARI

Kodirova Dilfuzaxon Abrorxonovna
Toshkent “Temurbeklar maktabi” HAL informatika fani o‘qituvchisi
https://www.doi.org/10.5281/zenodo.10485195

ARTICLE INFO

Received: 04th January 2024
Accepted: 10th January 2024
Online: 11th January 2024

KEY WORDS

Axborot xavfsizligi, kiberxavfsizlik, fishing, dastur, login, parol.

ABSTRACT

Ushbu maqolada informatika fanining “Axborot xavfsizligi” bo‘limini o‘qitishda bir necha tavsiyalar va tushunchalar berib o‘tilgan.

Yaqin yillarda hayotimizga oldinlari ko‘p ham e’tibor bermagan, biz ishlatmagan tushunchalar, yangi terminlar kirib keldi, ularni biz juda tez o‘zlashtirmoqdamiz. Axborot xavfsizligi, kiberxavfsizlik, fishing, pentesting, botlar, shubhali havolalar va xokazo. Axborotlar, ma’lumot bazalari bizni shunchalik o‘rab oldiki, u xatto yosh ham tanlayotgani yo‘q, oddiy telefon orqali biz ma’lumot bazasini ixtiyoriy yoshdagi insonni qo‘lida turganini ko‘rishimiz oddiy holga aylandi. Axborotlar bilan ishlash jarayoni tezlashgani, texnikaning, dasturiy ta’minotning odamlarning istaklaridanda tezroq o‘sib borayotgan bunga yaqqol misol. Sun’iy intellekt, sun’iy intellektning ham juda ko‘p yo‘nalishlari paydo bo‘lmoqda, uni hozirda hamma sohada ko‘rishimiz mumkin. Hamma narsaning ham ijobiy va salbiy jihatlari bo‘lgani kabi, texnika yangiliklari, bizni bunday davrda yanayam ehtiyorkorroq, axborotlarni himoyalash usullaridan foydalanishga ko‘proq chorlamoqda. Chunki turli tarmoqlar orqali kun ora kelib turgan shubhali havolalar, ulardan so‘ng “fake” xabarlar deb keladidan bildirishnomalar, shuniningdek, turli totanish insonlardan keladigan sms xabarlari, turli ogohlantirishlar bizni bu axborotlar davrida axborot hurujlaridan ehtiyot bo‘lishga chorlamoqda.

Axborot xavfsizligi (inglizcha: *Information security*, shuningdek, inglizcha: *InfoSec*) - axborotni ruxsatsiz kirish, foydalanish, oshkor qilish, buzish, o‘zgartirish, tadqiq qilish, yozib olish yoki yo‘q qilishning oldini olish amaliyotidir. Ushbu universal kontseptsiya ma’lumotlar qanday shaklda bo‘lishidan qat’iy nazar (masalan, elektron yoki, jismoniy) amal qiladi. Axborot xavfsizligini ta’minlashning asosiy maqsadi, ma’lumotlarning konfidensialligi, yaxlitligi va mavjudligini muvozanatli,qo‘llashning maqsadga muvofiqligini hisobga olgan holda va tashkilot faoliyatiga hech qanday zarar yetkazmasdan himoya qilishdir[1]. Bunga, birinchi navbatda, asosiy vositalar va nomoddiy aktivlar, tahdid manbalari, zaifliklar, potensial ta’sirlar va mavjud xavflarni boshqarish imkoniyatlarini aniqlaydigan ko‘p bosqichli

[1] Uz.Wekipedia.org

xavflarni boshqarish jarayoni orqali erishiladi. Bu jarayon xavflarni boshqarish rejasining samaradorligini baholash bilan birga olib boriladi.

Yurtimizda ham axborot xavfsizligin ta'minlash, kiberhujumlardan himoylanish, kiberxavfsizlikni rivojlantirish bo'yich bir qancha ishlar qilinmoqda,

Milliy kiberxavfsizlik strategiyasi, kiberxavfsizlik qonunchiligi, potensialni oshirish va ta'lim, aholini xabardor qilish kompaniyalari, hodisalarga javob berish va boshqalar. Ushbu qilinayotgan ishlar albatta, bizni, jamiyatimizni, axborotlar bilan ishlash xavfsizligimizni ta'minlash va oshirish uchun xizmat qilmoqda. Bu borada qilinayotgan ishlarga psixologik fishing, zararli dasturlardan foydalanmaslik va kiberxavflik qoidalariga amal qilish kabilarni misol tariqsida keltirishimiz mumkin[2].

Hakkerlar haqida eshitganmisiz? Ularning ham yaxshisi (White hat), yomoni (Black hat) va o'rta darajalisi (Grey hat) bo'ladi. Black hat hakkerlar odamlarni aldash, ularni pulini o'marish va turli yomon maqsadlarda ishlasa, "White hat" hakkerlari esa axborotlar xafvsizligini buzishga qilinayotgan harakatlarni aniqlab, ularga nisbatan chora ko'rilishi, "Black hat" hakkerlarni topish bilan shug'ullanadilar. "Grey hat" hakkerlar esa, ular havaskor hakkerlar sanaladi, ular turli sayt va tarmoq xavfsizligini tekshirish, uning zaif tomonlarini topib, bu haqda xabar berish bilan shug'ullanadilar va shu orqali pul ishlaydilar.

Axborot xavfsiligini ta'minlash bo'yicha bir necha tushunchalar kiritilgan. Ularga axborotni muhofazalash, axborot xavfsizligi, ma'lumotni ochish, identifikatsiya, autentifikatsiya, avrorizatsiya kabilar.

Axborotni muhofazalash - bu maiumotlarni o'g'irlash, yo'qotish, soxtalashtirish, qalbakilashtirsh, ruxsatsiz foydalanish va ko'paytirishning oldini olishga yo'naltirilgan tadbirlar majmuasidir[3].

Axborot xavfsizligi - foydalanish talablari asosida ma'lumotning yashirinligi, yaxlitligi va foydalanuvchanligini ta'minlashdir.

Ma'lumotni ochish - tasodifan yoki xusumatli harakatlar natijasida begona shaxsga axborotning mazmuni ruxsatsiz oshkor etilishdir.

Identifikatsiya - foydalanuvchini tizimga o'zini tanitish ^ jarayoni bo6lib, unda mijozning maxsus shaxsiy kartalaridan yoki uning biometrik xususiyatlaridan foydalaniladi

Autentifikatsiya - foydalanuvchining to'g'rilig» tekshiriladi 'N va uning asosida tizimda faoliyat olib borishi mumkinligi yoki mumkin emasligi beigiianadi.

Avtorizatsiya - foydalanuvchiga tizim tomonidan berilgan huquqlar majmuasidir.

Informatika va axborot texnologiyalari fanini "Axborot xavfsizligi" bo'limini o'qitishda bir necha tavsiyalarni ko'rib chiqaylik:

Axborot xavfsizligi ta'minlashning eng sodda tushunchalaridan boshlaydigan bo'lsak, ixtiyoriy sayt, ijtimoiy tarmoqdan ro'yxatdan o'tish jarayonida login va parollarni ishlatilishiga ahamiyat berish. Hozirgi kunda ro'yxatdan o'tish formalarini parollarga bir qancha talablar qo'yilgan, shu talablarni to'liq bajarish. Parol qo'yishda o'z shaxsiy ma'lumotlarimizdan foydalanmaslik, masalan tug'ilgan kunimiz, ism, familiya, yaqinlarimizni tug'ilgan kunlari, raqamlar va klaviaturadagi harflar ketma-ketligi kabilar. Bunday parollar eng oson Top-100 lik parollar ro'yxatiga kiradi, bunday parol qo'yishdan juda ko'p ko'p

[2] Kiberxafsizlik//taqdimot//Shermatov E.
[3] Informatika va axborot texnologiyalari// 11-sinf darsligi 91-95 betlar

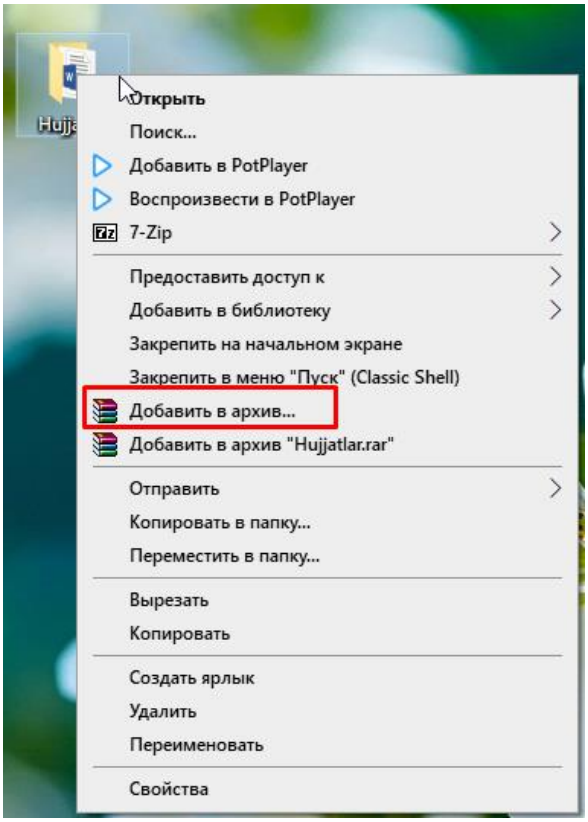
EURASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES
Innovative Academy Research Support Center
UIF = 8.3 | SJIF = 5.916 www.in-academy.uz

insonlar foydalaniladilar va kombinatsiya qilish jarayonida juda tez parolni buzilishiga olib keladigan sanaladi.

Kompyuter, mobil yoki texnik qurilmaga turli sinovlardan o‘tmagan dasturlarni o‘rnatishdan saqlanish kerak. Reklamalar orqali keladigan tekin dasturlar o‘zi bilan birgalikda viruslarni, troyanlarni, turli qurtlarni olib kelishiga hech kim javob bermaydi, shuning uchun bu qilayotgan hatti-harakatimizni o‘ylab amalga oshirishimiz kerakligini bildiradi. Turli viruslar uchun esa, antivirus dasturlaridan foydalanish, Windows operatsion tizimi foydalanuvchilari uchun esa, Sistema bilan birga o‘rnatiladigan Windows Defender dasturidan foydalanish va operatsion siztema bilan birgalikda yangilanib turish rejimini yoqpib qo‘yishimiz kerak bo‘ladi. Axborot ma’lumotlar bazalari o‘rab olgan dunyoda yashayotgan ekanmiz, eng ko‘p foydalanuvchilarga ega bo‘lgan messagelar, itimoiy tarmoq ilovalari (Instagramm, Telegram, Youtube, Tvitter…) da reklama qilinayotgan turli e’tiborni, qiziqishni uyg‘otayotgan xabarlardan ehtiyot bo‘lishimiz kerak. Hozirda xavaskor dasturlchilarning ko‘payib borayotgani, pul ishlash maqsadida, turli reklamalar, videolarni ommaga taqdim etish, ishga tushuvchi virus dasturlarni yaratish kabi videolar, kodlar yozishni o‘rgatish yosh avlod bunday narsalardan himoylashimiz zarurligini anglatadi. Axborot xavfsizligi haqida ko‘proq ma’lumot berish, barcha manbalardan to‘g‘ri foydalanishni o‘rganishimiz va bu haqida o‘quvchilarga ko‘proq ma’lumot berishimiz kerak.

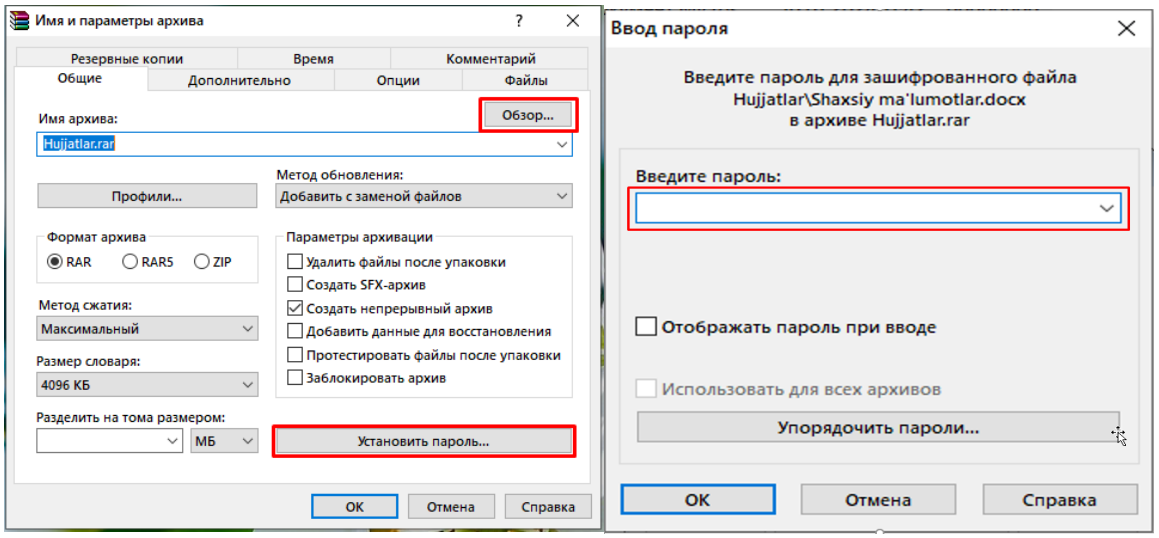
Axborotlarni himoya qilishning yana bir sodda usulini ko‘rib chiqaylik. Har qanday texnikadan foydalanuvchi o‘z shaxsiy ma’lumotlarini boshqalardan himoyalashga, fayllarini parollashga urinadilar. Bunday usullardan eng osoni bu arxivlash dasturlari yordamida (Winrar, WinZip, 7zip) amalga oshirishdir.

Keling buni qanday amalga oshirish ketma-ketligini ko‘rib chiqaylik:

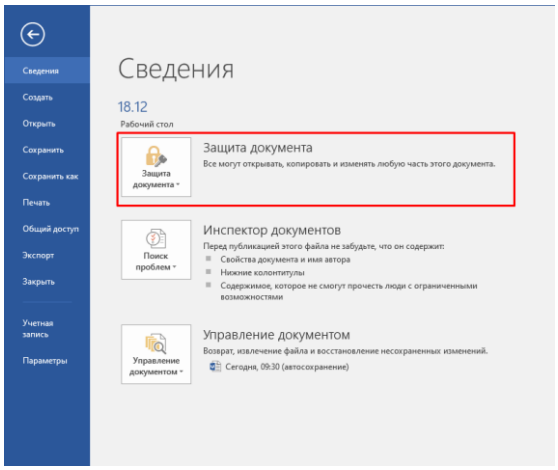


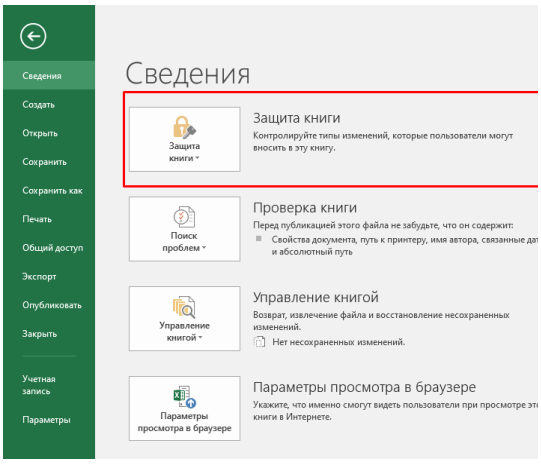
EURASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES
Innovative Academy Research Support Center
UIF = 8.3 | SJIF = 5.916 www.in-academy.uz

1. “Hujjatlar” deb yoki siz tomoningizdan ixtiyoriy nom bialn saqlangan fayl, papka tanlanadi.
2. Konteks menyu hosil qilinadi (sichqonchaning o‘ng tarafi bosiladi).
3. Hosil bo‘lgan “Имя и параметры архива” oynasidan “Обзор” tugmasi orqali saqlanadigan joyni ko‘rsatishimiz kerak bo‘ladi.
4. “Установить пароль” tugmasi orqali hujjatimizni shifrlaymiz.
5. Hosil bo‘lgan arxivlangan hujjatni ixtiyoriy vaqtda, parolni terib ishlatimishimiz mumkin.
6. Quyida qilinadigan amallar ketma-ketligi tasvirlarda ko‘rsatilgan.



Ko‘p foydaluvchiga ega bo‘lgan Office dasturlari paketining “Fayl” bo‘limining bir qancha buyruqlari yordamida ham himoya qilish mumkin.





Har bir imiz axborotlar bilan ishlash jarayonida axborotning mavjudligiga, ichinchligiga va xavfsizligiga e’tibor qaratishimiz, agar axborotlarga nixbatan Shubha uyg‘onsa kerakli organ mutaxassislariga murojaat qilishimiz talab etiladi.

References:

1. Informatika va axborot texnologiylari // 1-bosqich o‘quvchilari uchun uslubiy qo‘llanma//D.A.Kodirova // Ilm-ziyo//T:2023y.

2. Informatika va axborot texnologiyalari // Mustaqil tayyorgarlik uchun uslubiy qo‘llanma // D.A.Kodirova // Ilm-ziyo //T:2023y.
3. Kiberxafsizlik // Astrum IT Akademiyasi // Kiberxafsizlik // taqdimot // E.Shermatov
4. https//astrum.uz
5. www.youtube.com
6. www.scholargoogle.com