AXBOROT XAVFSIZLIGINING BUGUNGI KUNDA DOLZARBLIGI

A.Qodiriy nomli
Jizzax Davlat Pedagogika Universitetining
o'zbek tili va adabiyoti yo'nalishining
sirtqi 2-oliy ta'lim 4-kurs
2m1201-21 guruh talabasi

Samarqand viloyati Payariq tuman
3-son kasb-hunar maktabi
Informatika va maxsu fan o'qituvchisi
Mamaradjabova Xurshida Buriboyevna

Tel:+998 (93) 9633891
Xurshidamamaradjabova1991@gmail.com

Annotatsiya: Ushbu maqolada bugungi kunning dolzarb mavzularidan biri bo'lmish axborot xavfsizligining muammolari, axborotni himoyalash usullari keltirilgan.

Kalit so'zlar: axborot, innovatsion texnologiya, telekommunikatsion tizimlar, raqobatdoshlik, axborot xavfsizligi, axborotning yaxlitligi, viruslar.

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕГОДНЯ

Назван в честь А. Кадири
Джизакский государственный педагогический университет
Кафедра узбекского языка и литературы
Экстернат 2 ступени высшего образования
4 курса группы 2м1201-21

Пайарикский район Самаркандской области

Профессиональное училище №3
Учитель информатики и специальных наук
Мамараджабова Хуршида Бурибоевна

Телефон: +998 (93) 9633891
Хуршидамамараджабова1991@gmail.com

Аннотация: В данной статье представлены проблемы информационной безопасности, методы защиты информации, которые являются одной из актуальных тем современности.

Ключевые слова: информация, инновационные технологии, телекоммуникационные системы, конкурентоспособность, информационная безопасность, целостность информации, вирусы.

INFORMATION SECURITY ISSUES TODAY

Named after A. Kadiri
Jizzakh State Pedagogical University
Department of Uzbek language and literature
Externship 2nd stage of higher
education 4th year group 2m1201-21

Payarik district of Samarkand region
Vocational school No. 3
Teacher of computer science and special sciences
Mamarajabova Khurshida Buriboevna

Phone: +998 (93) 9633891
Khurshidamamarajabova1991@gmail.com

Abstract: This article presents problems of information security, methods of information protection, which are one of the pressing topics of our time.

Key words: information, innovative technologies, telecommunication systems, competitiveness, information security, information integrity, viruses.

Internet texnologiyalarining yaratilishi turli manbalardan tez va oson yo'l bilan axborot olish imkoniyatlarini hamma uchun-oddiy fuqarodan tortib yirik tashkilotlargacha misli ko'rilmagan darajada oshirib yubordi. Davlat muassasalari, fan-ta'lim muassasalari, tijorat korxonalari va alohida shaxslar axborotni elektron shaklda yaratib-saqlay boshladilar. Axborotdan samarali foydalanish imkoniyatlari axborot miqdorining tez ko'payishiga olib keldi. Biznes qator tijorat sohalarida bugun axborotni o'zining eng qimmatli mulki deb biladi. Bu albatta ommaviy axborot va hamma bilishi mumkin bo'lgan axborot haqida gap borganda o'ta ijobiy hodisa. Lekin maxfiy axborot oqimlari uchun Internet texnologiyalari qulayliklar bilan bir qatorda yangi muammolar keltirib chiqardi. Internet muhitida axborot xavfsizligiga tahdid keskin oshdi.

Axborot xavfsizligi tahdidlari turli belgilar orqali tavsiflanishi mumkin

- axborot yashirinligini buzish, asosan inson omili yoki muhofaza apparat ta’minoti faoliyatini izdan chiqarish;
- ma’lumotlar mazmunini o‘zgartirishga doir ruxsatsiz faoliyatlar orqali axborot yaxlitligiga zarar yetkazish;
- axborot foydalanuvchilariga kompyuter viruslari orqali tahdidlar;
- axborot xavfsizligiga ichki va tashqi tahdidlar;
- axborot xavfsizligi buzilishida global, hududiy va lokal tarmoqlar tahdidlari;
- Kompyuterga olisdan kirish - Internet yoki intranetga kimligini bildirmay kirishga imkon beruvchi dasturlar. O'zi ishlab turgan kompyuterga kirish: kompyuterga kimligini bildirmay kirish dasturlari asosida;

- Kompyuterni olisdan turib ishlatmay qo'yish - Internet tarmog’i orqali olisdan kompyuterga ulanib, uning yoki uni ayrim dasturlarining ishlashini to'xtatib qo'yuvchi dasturlar asosida(ishlatib yuborish uchun kompyuterni qayta ishga solish yetarli);
- Tarmoq skanerlari - tarmoqda ishlayotgan kompyuter va dasturlardan qay biri tajovuzga chidamsizligini aniqlash maqsadida tarmoq haqiqatda axborot yig'uvchi dasturlar vositasida;
- • Parol ochish - parollar fayllaridan oson topiladigan parollarni izlovchi dasturlar vositasida;
- Tarmoq tahlilchilari (snifferlar) - tarmoq trafikini tinglovchi dasturlar vositasida. Ularda foydalanuvchilarning nomlarini, parollarini, kredit kartalari nomerlarini trafikdan avtomatik tarzda ajratib olish imkoniyati mavjud.

  Eng ko'p yuz beradigan tajovuzlar quyidagi statistikaga ega:

  ✓ 1998 yili NIST tomonidan o'tkazilgan 237 kompyuter tajovuzining tahlili Internetda e'lon qilingan:

  - 9% tajovuzlar Windows muhitida yuz bergan. Saboq: Faqat Unixgina xatarli emas ekan.
  - 20% tajovuzlarda tajovuz qilganlar olisdan turib tarmoq elementlari(marshrutlovchilar, kommutatorlar, xostlar, printerlari brandmauer) gacha yetib borganlar.
  - Saboq: xostlarga olisdan turib bildirmay kirish bot-bot yuz beradi.
  - 5% tajovuzlar marshrutlovchilarga va brandmauerlarga qarshi muvaffaqiyatli bo'lgan.
  - Saboq: Internet tarmoq infrastrukturasi tashkil etuvchilarining kompyuter tajovuzlariga bardoshi yetarli emas.

- 4% tajovuzlarda Internetda tajovuzga bardoshi bo'sh xostlarni topish uchun uyushtirilgan.
- Saboq: Tizim administratorlarining o'zlari o'z xostlarini muntazam skanerlab turganlari ma'qul.
- 3% tajovuzlar web-saytlar tomonidan o'z foydalanuvchilariga qarshi uyushtirilgan.

Saboq WWWda axborot izlash xavfsiz emas.

2021 yilda:

- Norvegiyaning eng yirik gazetalari xakerlik hujumlari tufayli yopildi
- Hackerlar Dnevnik.ru saytini buzib, maktab o'quvchilarining baholarini o'zgartirdilar
- 1,6 million WordPress veb-saytlari hujumga uchradi
- Volvo avtomobillarini sindirish
- Xakerlar Qozog‘iston elektron hukumati saytiga virus dasturini yuklagan, uni foydalanuvchilar yuklab olgan
- Xakerlar Belarus pasportining IT tizimini buzishdi
- Luma Energy yirik energetika kompaniyasi kiberhujumlarga uchradi
- Dunyodagi eng yirik go'sht ishlab chiqaruvchi JBS kompaniyasiga xaker hujumi
- Xakerlar 2 yil davomida Belgiya Ichki ishlar vazirligi tarmog‘ida jimgina “o‘tirishdi” va xodimlarning xatlarini o‘qishdi.
- Avtomobil ehtiyot qismlari ishlab chiqaruvchi Toyota Auto Body kompaniyasiga kiberhujum
- Hackerlar Vashington politsiyasining IT tizimlariga buzib kirishdi va hujjatlarni o'g'irlashdi
- Kiberhujum tufayli Yaponiyaning barcha Toyota Motor zavodlarida ishlab chiqarish to'xtatildi

Tarmoqni kompyuter tajovuzlaridan himoyalash doimiy va o'z-o'zidan yechilmaydigan masaladir. Lekin qator oddiy himoya vositalari yordamida tarmoqqa suqulib kirishlarning ko'pchiligini oldini olish mumkin. Masalan yaxshi konfiguratsiyalangan tarmoqlararo ekran va harbir ish stantsiyalari(kompyuterlar)da o'rnatilgan virusga qarshi dasturlar ko'pchilik kompyuter tajovuzlarini barbod etadi. Axborot xavfsizligini ta’minlash uchun tashkiliy, texnik va dasturiy vositalardan foydalaniladi.

Tashkiliy vositalar tarkibiga texnik-tashkiliy va huquqiy-tashkiliy tadbir- lami kiritishimiz mumkin. Texnik-tashkiliy tadbirlarda xavfsizlik choralarini ta’minlash uchun ofis xonasidagi kompyuter, telefon, televizor, radio, signa- lizatsiya va shunga o‘xshash axborot chiqish ehtimoli bo‘lgan barcha vositalar ro‘yxatdan o‘tkaziladi.

Texnik vositalar elektron, elektromexanik va boshqa qurilmalardan iborat bo’lib, tizimlami texnik himoyalashda bevosita foydalaniladi. Keng im- koniyatli (0,01 - 1000 MHz) elektromagnit generatorlari kompyuter va boshqa uskunalardan chiquvchi qo‘shimcha to‘lqinlarini sezdirmaslik vazifasini o‘taydi

Axborotni yashirin olishga mo‘ljallangan mobil aloqa telefonlarini aloqa- dan uzish, elektr tarmog‘idan ma’lumot chiqmasligini ta’minlovchi filtrlar, diktofonlami kuchli elektromagnit to‘lqinlar bilan ishdan chiqaruvchi vositalar qo‘llaniladi

Dasturiy vositalar tarkibiga axborot xavfsizligi, foydalanuvchilar shaxsini identifikatsiyalash, kirish nazorai n o‘matish, ma’lumotlarni yashirin ko‘ri- nishga keltirish kabi vazifalami bajarishga mo‘ljallangan maxsus dasturiy vositalar tizimi kiradi.

Axborotni himoyalovchi dasturiy vositalaming tarkibi quyidagilardan iborat:

• bir necha fayl yoki jildlami yig‘ish orqali ulaming hajmini keskin ka- maytiiib tashqi ta’sirlardan himoyalash dasturlari;

• kompyuter tizimiga beruxsat kirishdan himoyalash dasturlari;

• tizimni viruslardan himoyalashga mo‘ljallangan antivims dasturlari;

• ma’lumotlar yashirinligini ta’minlovchi kdptografik dasturlar.

Windows 7 operatsion tizimini himoyalash.

Bajarish:

1. Пуск tugmasini faollashtirish orqali Панель управления bo‘limi- dan Учетные записы пользователей и сем... qismiga kiriladi va u yerdan Учетные записы пользователей bandi faollashtiriladi;

2. Внесение изменений в учетную запись пользователя oynasidan Изменение своего пароля muloqot darchasiga kiriladi;

3. Agar kompyuterga oldin parol qo‘yilgan bo'Isa, Текущей пароль qa- toriga oldingi parol kiritilib, so‘ngra Новый пароль va Подтверждение пароля qatoriga yangi parol kiritiladi:

Ushbu ketma-ketlik bajarilgandan so‘ng, kompyuter ishga tushirilganda yangi parol bilan kirish zarur bo‘ladi.

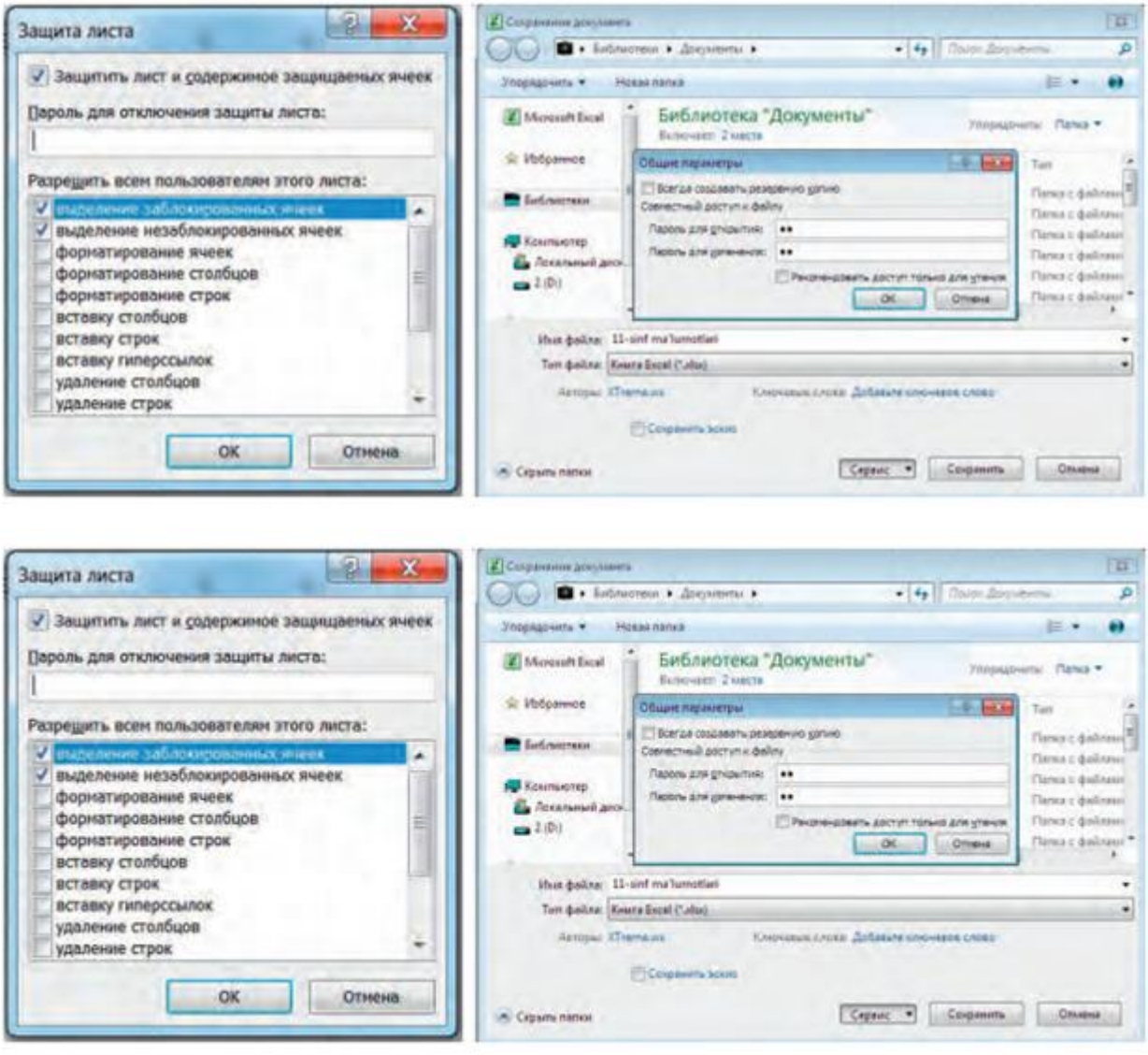
MS Excel 2010 elektron jadvalida ma’lumotlami himoyalash.

Bajarish:

1. MS Excel 2010 ning menyusida Рецензирование tasmasi faollashtiriladi;

2. Tasmaning Защитить лист bandi bosiladi. Natijada ekranda Защита листа muloqot oynasi paydo bo'ladi. Hosil bo‘lgan oynaning Пароль для отключения защиты листа qatoriga parol kiritiladi;

Himoyalangan varaqdagi ma’lumotlami o‘zgartirish uchun MS Excel 2010ning menyusidan ецензирование tasmasi faollashtiriladi. Tasmaning Изменение qismidan Снять Защитить листа bandi tanlanadi. Natijada Снять Защитить листа muloqot oynasi paydo bo‘ladi. Ushbu hosil bo‘lgan oynaning ma’lumot kiritish qatoriga oldin himoyalangan parol kiritiladi.



Foydalanilgan adabiyotlar:

1. Маллабоев Н., Шокиров Д. СПОСОБЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ //Теория и практика современной науки. – 2016. – №. 6-1. – С. 826-830.

2. Маллабоев Н., Шокиров Д. СИСТЕМЫ ЭЛЕКТРОННОГО ПЛАТЕЖА //Теория и практика современной науки. – 2016. – №. 6-1. – С. 830-834.

3. Abdullaeva N., Mamurova F., Mallaboev N. EFFICIENCY OF EXPERIMENTAL PREPARATION USE MULTIMEDIA TO ENLARGE SOME QUESTIONS //Экономика и социум. – 2020. – №. 6. – С. 11-13.

4. S.K. Ganiyev, M.M. Karimov, K.A. Tashev Axborot xavfsizligi “Aloqachi” - 2008

5. Axborot xavfsizligi [Matn]: o’quv qo’llanma /Sh.B.Sayfullayev. –Toshkent: “Turon nashriyot”, 2021.-140 b