MUHAMMAD AL-XORAZMIY
NOMIDAGI TATU FARG'ONA FILIALI

FERGANA BRANCH OF TUIT
NAMED AFTER MUHAMMAD AL-KHORAZMI

"AL-FARG'ONIY AVLODLARI"

ELEKTRON ILMIY JURNALI | ELECTRONIC SCIENTIFIC JOURNAL

TA'LIMDAGI ILMIY, OMMABOP VA ILMIY TADQIQOT ISHLARI

3-SON 1(3)
2023-YIL

TATU, FARG'ONA
O'ZBEKISTON

ISSN 2181-4252

O‘ZBEKISTON RESPUBLIKASI RAQAMLI TEXNOLOGIYALAR VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI FARG‘ONA FILIALI

Muassis: Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Farg‘ona filiali.
Chop etish tili: O‘zbek, ingliz, rus.
Jurnal texnika fanlariga ixtisoslashgan bo‘lib, barcha shu sohadagi matematika, fizika, axborot texnologiyalari yo‘nalishida maqolalar chop etib boradi.

Учредитель: Ферганский филиал Ташкентского университета информационных технологий имени Мухаммада ал-Хоразми.
Язык издания: узбекский, английский, русский.
Журнал специализируется на технических науках и публикует статьи в области математики, физики и информационных технологий.

Founder: Fergana branch of the Tashkent University of Information Technologies named after Muhammad al-Khorazmi.
Language of publication: Uzbek, English, Russian.
The magazine specializes in technical sciences and publishes articles in the field of mathematics, physics, and information technology.

2023 yil, Tom 1, №3
Vol.1, Iss.3, 2023 y

ELEKTRON ILMIY JURNALI **ELECTRONIC SCIENTIFIC JOURNAL**

«Al-Farg‘oniy avlodlari» («The descendants of al-Fargani», «Potomki al-Fergani») O’zbekiston Respublikasi Prezidenti administratsiyasi huzuridagi Axborot va ommaviy kommunikatsiyalar agentligida 2022-yil 21 dekabrda 054493-son bilan ro’yxatdan o’tgan.

Tahririyat manzili:
151100, Farg‘ona sh., Aeroport ko‘chasi 17-uy, 201A-xona
Tel: (+99899) 998-01-42
e-mail: info@al-fargoniy.uz
Qo‘lyozmalar taqrizlanmaydi va qaytarilmaydi.

FARG’ONA - 2023 YIL

TAHRIR HAY'ATI

Jurnal quyidagi bazalarda indekslanadi:

MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

XAVF-XATARLARNI KELTIRIB CHIQARUVCHI OMILLAR, XAVF-XATARLARNI ANIQLASH USULLARI, MUAMMO VA YECHIM

Muxtarov Farrux Muhammadovich,

Muhammad al-Xorazmiy nomidagi

TATU Farg‘ona filiali dotsenti

Annotatsiya: Ushbu maqolada xavf-xatarlarni keltirib chiqaruvchi omillar nazariy jihatdan olib borilgan ilmiy hulosalarga ko‘ra o‘rganib chiqilgan. Xavflarni turlariga qarab xavf-xatarlarni aniqlash usullari bayon etilgan. Umumiy xavf-xatarlarni tahlil qilgan holda ularni oldini olish va oqibatlarini yumshatish borasida xavf-xatarlarni baholagan holda bir necha yechimlar taqdim etilgan.

Kalit so‘zlar: risk, tahdid, zaiflik, autentifikatsiya, shifrlash, deshifrlash, kiber-hujum, aktiv, dasturiy ta’minot, sun’iy tahdid, tabiiy tahdid, geofizik hodisalar, geologik hodisalar.

Kirish. Har qanday tizim yoki maxsus kanallarda xavf-xatarlarni aktiv, zaifilik va tahdid keltirib chiqaradi. Aktiv tarmoq va unda o‘tadigan ma’lumotlar va ularni qiymatini belgilovchi qimmatliklardir. Biror ma’lumotni hinoyalash uchun albatta ular qandaydir qiymatga ega bo‘lishi kerak. Zaifilik maxsus kanaldagi nuqson yoki kamchilik deb tushunilsa, tahdid esa aynan shu zaiflikdan foydalanib amalga oshishi mumkun bo‘lgan zararli hodisa hisoblanadi. Hech qanday texnologiya, tizim yoki alohida dasturlar yoki biror qiymatga ega bo‘lgan ma’lumotlar bir so‘z bilan aytganda aktivlar zaiflikdan holi bo‘lmaydi. Shunday ekan doimo tahdidlar ham mavjud bo‘ladi. Bu uch narsa ya’ni aktiv, zaiflik, tahdid xavf-xatarlarni kelib chiqishini asosiy, tarkibiy qismi hisoblanadi. Mavjud zaifliklarni bartaraf etmasdan va tahdidlarga aniqlab, ularga qarshi kurashmasdan turib xavf-xatarlarni oldini olish mumkun emas. Quyida mavjud zaifliklar, tahdid turlari va uni aniqlash usullari bilan tanishamiz.

Zaiflik bu tajovuzkorlar tomonidan ishlatilishi mumkin bo‘lgan axborot aktivi yoki boshqarish vositalarining zaif tomonlari. Boshqacha qilib aytganda, biz axborot xavfsizligiga potentsial salbiy ta'sir ko‘rsatishi mumkin bo‘lgan axborot vositasi yoki tizimini yaratish/konfiguratsiya/foydalanishdagi kamchiliklar yoki xatolar haqida bormoqda.

Shuni ta'kidlash kerakki, axborot xavfsizligi zaifligi o‘z-o‘zidan xavfli emas. Ular faqat axborot xavfsizligiga tahdidlarni amalga oshirish imkoniyatlarini ochib beradi. Zaifliklarning eng keng tarqalgan sabablari, qoida tariqasida, quyidagilarni o‘z ichiga oladi: dasturiy ta'minotni loyihalash va ishlatishdagi xatolar; dasturiy ta'minotni ruxsatsiz joriy etish va undan keyin foydalanish; zararli dasturlarni joriy etish; inson omili.

Axborot xavfsizligi zaifliklarining juda ko‘p tasniflari mavjud. Masalan, ular obyektiv (dasturiy ta'minotning texnik xususiyatlarining o‘ziga xos xususiyatlaridan kelib chiqqan holda), sub'ektiv (dasturiy ta'minotni ishlab chiquvchilar va foydalanuvchilarning, tizim ma'murlarining harakatlari tufayli) va tasodifiy (kutilmagan holatlar tufayli) bo‘linadi. Boshqa tasniflash zaifliklarning quyidagi turlarini belgilaydi: texnologik yoki arxitektura, zarur axborot xavfsizligi texnologiyalari mavjud bo‘lmaganda ifodalangan; tashkiliy, axborot xavfsizligini ta'minlashning o‘rnatilgan va tartibga solinadigan tartiblari yo‘qligida ifodalangan; operatsion, tashkilotning axborot tuzilmasi kamchiliklari bilan bog‘liq.

Adabiyotlar tahlili va metodologiya. Ushbu maqolani yozishda bir qancha mavzuga oid adabiyotlar, ilmiy maqolalar o‘rganib chiqilgan. Ularni orasida axborot tizimlariga tahdidlarni tadqiq qilishda F.Muxtorov, A.Umarov, A.Ro‘zaliyevlarning “Axborot tizimlarida xavfsizlik tahdidlarining tasnifi”[1] va D.Tojimatov, J.Mirzayevlarning “Use of Artificial Intelligence Opportunities for Early Detection of Threats to Information Systems”[2] maqolalari, xavf-xatarlarni aniqlash, baholash va boshqarishni tashkil qilishda F.Muxtarovning “Axborot xavfsizligi xavflarini tahlil qilish uchun ierarxik aktivlarni baholash usuli”[3] maqolasi tarmoq

https://doi.org/10.5281/zenodo.8317695

https://journals.indexcopernicus.com/search/article?articleId=3712367

https://al-fargoniy.uz/

xatoliklari haqida ma’lumot olishda Kamolovich B. E. “Tarmoqlarda uzatiladigan ma’lumotlarni xatoliklarini bartaraf etish usullari”[4] maqolasi o‘rganilib, ulardan iqtiboslar keltirilgan.

Natijalar. Tahdid tushunchasi. Ma’lumki tahdidlar tabiiy va sun’iy turlarga bo‘linadi. Axborot xavfsizligi sohasida tahdidlarni o‘rganish juda muhum hisoblanib, maxsus kanallarga bo‘ladigan ehtimoliy xavf-xatarlarni bartaraf etish aynan tahdidni aniqlash va uni darajasini to‘g‘ri baholagan holda ta’sirini kamaytirishga bog‘liq.

Tabiiy tahdid tabiat hodisalari tufayli vujudga kelishi ehtimolligi yuqori bo‘lgan favqulotda vaziyatni keltirib chiqaradigan jarayon hisoblanadi. Tabiiy xavf manbalari (tashuvchilari) litosfera, gidrosfera, atmosfera va kosmosning turli xil noqulay tabiiy jarayonlar sodir bo‘ladigan va xavfli tabiat hodisalarining yuzaga kelishi mumkin bo‘lgan qismlaridir.

Tabiiy favqulodda vaziyatlarning manbalari bo‘lgan xavfli tabiat hodisalarini quyidagilarga bo‘lish mumkin:

- xavfli geofizik hodisalar (zilzilalar, vulqon otilishi);

- xavfli geologik hodisalar (ko‘chkilar, eroziya, qiyaliklarning yuvilishi, qurumlar);

- xavfli gidrometeorologik hodisalar, shu jumladan meteorologik (bo‘ronlar, dovullar, tornadolar, juda kuchli qor, jala, yomg‘ir, tumanlar, qattiq sovuq, issiqlik), agrometeorologik (ayozlar, quruq shamollar, tuproq va atmosfera qurg‘oqchiligi), gidrologik (suv toshqini, muzliklar, tirbandliklar, sellar), dengiz gidrologik va geliogeofizik xavflar (kuchli magnit bo‘ronlar, qisqa to‘lqinli aloqaning uzilishi bilan ionosferada kuchli buzilish radiatsiyaviy vaziyat) va asteroid-kometa xavfi;

- tabiiy yong‘inlar.

Odatda tabiiy tahdidlar kiber tahdid hisoblanmaydi ammo favqulotda vaziyat sodir bo‘lganda uning korxona-tashkilotlarning axborot tizimlari uchun keltiradigan zarari kiber hujumnikidan ancha yuqori bo‘lishi mumkun.

Tabiiy tahdidlar axborot tizimlariga tog‘ridan-to‘g‘ri tasiri kam hisoblanib, asosan tizim o‘rnatilgan qurilmalarni vayron qilish orqali zarar keltiradi. Shu sababli xavfsizlik tizimlarini ishlab chiqishda tabiiy tahdidlarni aniqlash va favqulotda vaziyatni oldini olishga qaratilgan chora tadbirlar ko‘rilishi maqsadga muofiq hisoblanadi.

Sun’iy tahdidlar bevosita shaxsga bog‘liq bo‘lib, tasodifiy yoki qasddan uyushtirilgan tahdidlar turlariga bo‘linadi.

Tasodifiy tahdidlar ehtiyotsizlik, beparvolik, bilimsizlik, sinalmagan hodimni ishga qabul qilish, texnik va dasturiy tizimlardagi xatolik tufayli vujudga keladi. Bunday tahdidlar maqsadsiz hisoblanib korxona-tashkilot uchun keltiradigan zararini oldindan aniqlash qiyin hisoblanadi.

Qasddan uyushtirilgan tahdidlar aniq maqsadga qaratilgan bo‘lib, ichki va tashqi tahdid turlariga bo‘linadi. Ichki tahdidlarga asosan yollanma josuslar, qasd olish maqsadidagi hodim havflari kiradi. Tashqi tahdidlarga esa ehtimoliy kiber hujumlar va kompyuter viruslari havfi kiradi. Qasddan uyushtirilgan tahdidlar korxona-tashkilot axborot tizimlarini yo‘q qilish, barqaror ishlashini izdan chiqarish, ma’lumotlarni o‘girlash, nusxa ko‘chirish, o‘zgartirish kabi maqsadlarga qaratilgan bo‘ladi.

Tahdidlarni ta’sirini kamaytirish usullari. Har qanday qimmatli aktivga ega korxona tashkilorlar axborot tizimlarini potensial tahdidlardan himoyalashda turli fizik va apparat-dasturiy vositalardan foydalangan holda xavfsizlik usullaridan foydalanishadi. Fizik himoya usullari va vositalariga misol tariqasida qo‘riqlanadigan (sim to‘siq, balan beton devor) hudud, bardoshli obekt (bino), qo‘riqlash hizmati (qorovul, xavfsizlik hodimi), kuzatuv kameralari, signalizatsiya vositalari, axborot tizimi uchun alohida ajratilgan himoyalangan xona, eshik qulflari, o‘t o‘chirish vositalari, vintelatsiya vositalari, isitish yoki sovitish tizimlari kiradi. Apparat-dasturiy vositalar bevosita axborot tizimlari va u o‘rnatilgan kompyuterlarga bog‘lanadi. Bularga tarmoqlararo ekran vositalari, tarmoq marshrutizatorlari, komutatorlar, antivirus dasturlari, tarmoq analizatorlari, ddos hujumlariga qarshi vositalar va axborot tizimida foydalaniladigan kriptografik usullar, autentifikatsiya usullari, rollarga asoslangan usullarni misol sifatida keltirishimiz mumkun.

Axborotni tizimlarini himoyalashga qaratilgan barcha mavjud usullar hozirda bardoshli hisoblansada, ular tahdidlar avvaldan mavjud bo‘lgan hollarda yoki

https://doi.org/10.5281/zenodo.8317695

https://journals.indexcopernicus.com/search/article?articleId=3712367

https://al-fargoniy.uz/

tahdid yuzaga kelganda uni aniqalash imkoniyatiga ega. Qolaversaga bunday vositalarni boshqarish inson omiliga bog‘liq bo‘lib qolmoqda. Bu esa axborot tizimlariga qaratilgan tahdid turlarini ajratib olish va himoya uchun usullarini tanlashda qaror qabul qilish vaqt yo‘qotilishiga olib keladi. Bazida to‘g‘ri himoya tizimlari tahdid ro‘y bergandan keyin o‘rnatiladi. Bungacha esa tahdidlar axborot tizimlariga zarar yetkazgan bo‘ladi. Hozirda hackerlar ko‘plab hujumlarda sun’iy intelektni keng qo‘llab kelmoqdalar. Bu mavjud tizimlarni bardoshlilik darajasini zaif holga keltirmoqda. Mashinani o‘qitish tizimlari orqali neyron tarmoqlar himoya tizimlarini mukkammal o‘rganadi va ularni zaif tamonlarini ochib beradi. Ayrim hollarda sohta tahdid yaratib himoya tizimlarini chalg‘itishga harakat qiladi.

Tahdidlarni erta aniqlash bizga tahdid turini hususiyatlarini o‘rganish, u keltirib chiqaradigan oqibatini baxolash va unga qarshi zaruriy choralarni ko‘rish imkoniyatini taqdim etadi. Lekin axborot tizimiga bo‘ladigan kiber tahdidlar sodir bo‘lishiga nisbatan ancha yuqori tezlikda amalga oshadi. Chunki kompyuterda axborot almashuv va hisoblash tezligi inson omilidan yuqori hisoblanadi. Shu sababdan sun’iy intelekt orqali tahdidlarni erta aniqlash tahdidlarni turini tez va to‘g‘ri baholashga va ularga qarshi himoya vositalarini to‘g‘ri tanlashga yordam berishi mumkun. Bu albatta sun’iy intelekt imkoniyatlaridan foydalangan holda alohida aqlliy xavfsizlik tizimini ishlab chiqishni va bu tizimga korxona-tashkilotlarni axborot tizimlarini integratsiya qilishni talab qiladi.

Muhokama. Xavf-xatar kiberxavfsizlikka oid bo‘lgan tushunchalardan biri hisoblanadi. Quyida risk tushunchasi va uni boshqarish bo‘yicha batafsil ma’lumotlar keltirilgan. Xavf-xatar kiberxavfsizlik lug‘atida “RISK” deb yuritiladi.

Risk - belgilangan sharoitda tahdidning manbalarga bo‘lishi mumkin bo‘lgan zarar yetkazilishini kutish. Bundan tashqari, riskni quyidagicha tushunish mumkin:

- Risk - ichki yoki tashqi majburiyatlar natijasida tahdid yoki hodisalarni yuzaga kelishi, yo‘qotilishi yoki boshqa salbiy ta’sir ko‘rsatishi mumkin bo‘lgan hodisa.
- Risk - manbaga zarar keltiradigan ichki yoki tashqi zaiflik tahdidi bo‘lishi ehtimoli.
- Risk - hodisa sodir bo‘lishi ehtimoli va ushbu hodisaning axborot texnologiyalari aktivlariga ta’siri.

Risk, tahdid, zaiflik va ta’sir tushunchalari o‘rtasida o‘zaro bog‘lanish mavjud bo‘lib, ularni quyidagicha ifodalash mumkin:

RISK = Tahdid x Zaiflik x Ta’sir

Boshqa tomondan, hodisaning axborot texnologiyalari aktiviga ta’siri - aktivdagi yoki manfaatdor tomonlar uchun aktivning qiymatidagi zaiflikning natijasi, ya’ni:

RISK = Tahdid x Zaiflik x Aktiv qiymati

Risk o‘zida quyidagi ikkita omilni mujassamlashtiradi:

- zararli hodisaning yuzaga kelishi ehtimoli;
- va zararli hodisa oqibatlarining ehtimoli.

Risk ta’siri. Risk normal amalga oshirish jarayoniga va loyiha narxiga yoki kutilgan qiymatga ta’sir etadi. Risk ta’siri tashkilot, jarayon yoki tizimga zararli muhit sababli yuzaga keladi. Ta’sir riskning kuzatilishi ehtimoli jiddiyligini ko‘rsatadi. Bizning holatda kanallar uzilishi holati jiddiy deb baholanadi.

Risk chastotasi. Riskni aniqlash va baholash nuqtai nazaridan risklarni tasniflashda ularning takrorlanish chastotasiga va ko‘p sonliligiga asoslanadi. Chastota va ko‘p sonlilik risklarni monitoringlashda muhim hususiyat hisoblanib, risklar ikki guruhga: minor risklar - e’tibor talab qilmaydigan va major risklar - alohida e’tibor va kuzatuv talab qiluvchilarga ajratiladi. Bu holatdabizning riskimiz minor risklar tavsifiga kiradi.

Risk darajasi. Risk darajasi tarmoqga (yoki tizimga) natijaviy ta’siming bahosi bo‘lib, quyidagi tenglik bilan ifodalanadi:

Risk darajasi = natija * ehtimollik

https://doi.org/10.5281/zenodo.8317695

https://journals.indexcopernicus.com/search/article?articleId=3712367

https://al-fargoniy.uz/

Risk darajalari 4 ta: ekstremal yuqori, yuqori, o‘rta va past. Kanal uzulishlarini biz yuqori darajali risklar toifasiga kiritamiz.

Ekstremal yuqori yoki *yuqori risk* paydo bo‘lishini va salbiy ta’sirini kamaytirish maxsus yo‘naltirilgan qarshi choralarni talab etadi. Bu darajadagi risklar yuqori yoki o‘rtacha ta’siming yuqori ehtimolligiga ega bo‘ladi. Mazkur darajadagi risklar jiddiy xavfga sabab bo‘ladi va shuning uchun, zudlik bilan aniqlash hamda qarshi chora ko‘rish talab etiladi.

O‘rta darajali risklar yuqori ehtimollikka ega past natijali hodisa yoki past ehtimollikka ega yuqori natijali hodisa bo‘lishi mumkin. Alohida qaralganida, yuqori ehtimollikka ega past natijali hodisalar loyiha narxiga yoki kutilgan natijaga kam ta’sir qiladi. Past ehtimollikka ega yuqori natijali hodisalar doimiy monitoringni talab etadi. O‘rta darajali risklarga zudlik bilan chora ko‘rish talab etilmasada, himoyani dastlabki vaqtda o‘matish talab etiladi.

Past darajali risklar odatda e’tibor bermasa bo‘ladigan yoki keyingi baholashlarda e’tibor bersa bo‘ladigan risklar toifasi bo‘lib, ularni bartaraf etish qisqa muddatda amalga oshirilishni talab qilmaydi yoki ortiqcha sarf xarajatga sabab bo‘lmaydi.

Risk matritsasi risklarni paydo bo‘lish ehtimolini ularning natijasi va ta’siri orqali aniqlaydi hamda risk jiddiyligini va unga qarshi himoya chorasi sathini grafik taqdim etadi. Risk matritsasi riskning ortib boruvchi ko‘rinishi uchun foydalaniluvchi sodda jarayon bo‘lib, qarshi choralarni ko‘rishda yordam beradi. Risk matritsasi risklarni turli darajalarda aniqlash va jiddiylik nuqtai nazaridan guruhlash imkonini beradi (1-jadval).

Ehtimollik (ravshan)		Oqibat/ ta’sir					
			Muhim emas	Kam	O‘rta	Ko‘p	Jiddiy
81-100%	Ehtimollik (noravshan)	Juda yuqori	Past	O‘rta	Yuqori	O‘ta yuqori	O‘ta yuqori
61-80%		Yuqori	Past	O‘rta	Yuqori	Yuqori	O‘ta yuqori
41-60%		Teng	Past	O‘rta	O‘rta	Yuqori	Yuqori
21-40%		Past	Past	Past	O‘rta	O‘rta	Yuqori
1-20%		Juda past	Past	Past	O‘rta	O‘rta	Yuqori

1-jadval. Risk matrisasi

Xulosa. Xulosa qilib aytadigan bo‘lsak xavf-xatarlarni keltirib chiqadigan omillarni ikkta kata guruhlarga bo‘lib o‘rganiladi. Birinchisi tabiiy tahdid omillari, ikkinchisi sun’iy tahdid omillari hisoblanadi. Tabiiy tahdid keltirib chiqaruvchi omillar bevosita tabiyat hodisalariga bog‘liq hisoblanib, bu sohada o‘rganish, tahlil qilish va bularga qarshi choralar ko‘rish davlat nazoratidagi tashkilotlar va ilmiy markazlar zimmasiga yuklatiladi. Sun’iy xavf-xatarlarni keltirib chiqaruvchilar bevosita har bir korxona tashkilolarni individual faoliyatidan kelib chiqadi. Bu omillarni aniqlash va ularga qarshi choralar ko‘rish korxona va tashkilotlarni talabiga ko‘ra axborot xavfsizligi sohasi mutaxassislarining tajribalaridan kelib chiqib amalga oshiriladi. Maqolada bayon qilinganidek xar-qanday xavf-xatarni keltirib chiqaruvchi omillar korxona va tashkilotning ish potensiyaliga salbiy ta’sir o‘tkazadi. Shu sababdan xavf-xatarlarni past, o‘rta, yuqori darajalarini aniqlashda risklarni boshqarish va baholash usullaridan foydalanish xavf-xatarlar keltirib chiqaradigan zararni bo‘lmasligi yoki oqibatni yengillashtirishni yagona yechimi sifatida qaraladi.

Foydalanilgan adabiyotlar

[1]. F.Muxtorov, A.Umarov, A.Ro‘zaliyev “AXBOROT TIZIMLARIDA XAVFSIZLIK TAHDIDLARINING TASNIFI”., “Engineering problems and innovations” ilmiy jurnali

[2]. Dostonbek T., Jamshid M. Use of Artificial Intelligence Opportunities for Early Detection of Threats to Information Systems //Central Asian Journal of Theoretical and Applied Science. – 2023. – Т. 4. – №. 4. – С. 93-98.

[3]. MIRZAYEV J. B., TOJIMATOV D. H. O. G. L. I. KIBERXAVFSIZLIKNI TA’MINLASH, KIBERHUJUMLARNI OLDINI OLISH BO‘YICHA DAVLAT SIYOSATI YURITILISHI //ИНТЕРНАУКА Учредители: Общество с ограниченной ответственностью" Интернаука". – С. 36-37.

[4]. Muxtorov F. M. et al. AXBOROT XAVFSIZLIGI XAVFLARINI TAHLIL QILISH

https://doi.org/10.5281/zenodo.8317695

https://journals.indexcopernicus.com/search/article?articleId=3712367

UCHUN IERARXIK AKTIVLARNI BAHOLASH USULI //INTERNATIONAL CONFERENCES. – 2022. – T. 1. – №. 4. – C. 76-80.

[5]. Kamolovich B. E. TARMOQLARDA UZATILADIGAN MA’LUMOTLARNI XATOLIKLARINI BARTARAF ETISH USULLARI //Scientific Impulse. – 2022. – T. 1. – №. 4. – C. 1637-1640.

[6]. Tojimatov D. X. Kiberxavfsizlik: tahdilar, muammolar, yechimlar,“ //Axborot-kommunikatsiya texnologiyalari va telekommunikatsiyalari sohasida zamonaviy muammolar va yechimlar” Respublika Ilmiy-texnik anjumani TATU Farg ‘ona filiali. – 2022.

[7]. Tojimatov D. u KIBER TAHDIDLARNI BASHORAT QILISH VA XAVF-XATARLARDAN HIMOYALANISHDA SUN’IY INTELEKT IMKONIYATLARIDAN FOYDALANISH: DX Tojimatov. Katta o ‘qituvchi, TATU Farg’ona filiali //Потомки Аль-Фаргани. – 2023. – Т. 1. – №. 2. – С. 41-44.

https://doi.org/10.5281/zenodo.8317695

https://journals.indexcopernicus.com/search/article?articleId=3712367

https://al-fargoniy.uz/