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

2-SON 1(2)
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, №2
Vol.1, Iss.2, 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

MAXSUS AXBOROT ALMASHUV KANALLARIGA BO‘LADIGAN XAVF-XATARLARNI ANIQLASH, BAHOLASH VA BOSHQARISH HAMDA ULARNI BARTARAF ETISH USULLARINI ISHLAB CHIQISH

Muxtarov Farrux Muhammadovich,

TATU Farg‘ona filiali dotsenti.

Annotatsiya: Ushbu maqolada korporativ tarmoq asosida qurilgan maxsus axborot almashuv kanallarida yuz berishi mumkun bo‘lgan xavf-xatarlarni aniqlash, baholash va boshqarish usullari tadqiq qilingan. Maxsus kanallarni xavf-xatarlarga bardoshli qilish hamda ularni barqaror ishlashini ta’minlash uchun tarmoq xavfsizligi protokollari va texnologiyalari asosida xavlarni bartaraf etish usullari ishlab chiqilgan. Ishlab chiqilgan usullarni amaliyotga tadbiq qilish borasida ijobiy natijalar olingan.

Kalit so‘zlar: kanal, VPN (Virtual hususiy tarmoq), STP (Zaxiralash protokoli), LACP (kanallarni agregatlash protokoli), risk, tahdid, zaiflik, autentifikatsiya, shifrlash, deshifrlash, DDOS, firewall.

Kirish. Maxsus kanal bu – kompyuter tarmoqlari orqali axborot almashishda korporativ tarmoq uchun asosni tashkil etuvchi maxsus ajratilgan, himoyalangan aloqa liniyasi xisoblanadi. Aloqa liniyalari odatda elektron axborot signallari uzatiladigan fizik qurilma, ma'lumotlarni uzatish texnologiyalari va oraliq qurilmalaridan iborat bo‘ladi. Raqamli ma’lumotlarni uzatish asosan simli va simsiz tashkil etilgan aloqa liniyalari orqali amalga oshiriladi. Har qanday tarmoq texnologiyasi aloqa liniyalari orqali diskret ma'lumotlarning ishonchli va tezkor uzatilishini ta'minlashi kerak. Texnologiyalar o‘rtasida katta farqlar mavjud bo‘lsada diskret ma'lumotlarni uzatishning umumiy tamoyillariga asoslanadi. Ushbu tamoyillar turli xil fizik tabiatdagi aloqa liniyalarida impulsli yoki sinusoidal signallardan foydalangan holda ikkilik va nollarni ifodalash usullari, xatolarni aniqlash va tuzatish usullari, siqish usullari va almashtirish usullarini o‘z ichiga oladi.

Hozirda davlatlararo munosabatlarda, davlat va nodavlat korxona-tashkilotlarida, shaxsiy ma’lumotlar almashishda uzluksizlikni ta’minlash, axborotlarni o‘g‘irlanishi, yo‘q qilinishi, o‘g‘irlanishi kabi xavflarni oldini olishda maxsus kannallar qurish hamda ulardan foydalanish keng qabul qilingan standartga aylanib bormoqda[2]. Maxsus kanal o‘z tuzilishiga ko‘ra himoyalangan tarmoq sifatida qaralsada, lekin bundan tarmoqlarni ham ma‘lum zaifliklari mavjud. Yuqorida keltirib o‘tilgan turli sohalarni texnik xizmatlarining barchasi tunellashga asoslangan maxsus kanallar hisoblanadi. Bu bir biriga misoli o‘rgimchak to‘ridek chambarchas bog‘langan kanallardan foydalanib ikki jo‘natuvchi va qabul qiluvchi tamonning virtual yo‘lak hosil qilishidek gap. Hozirgi kunda VPN (Virtual private network) tarmog‘i texnologiyasi aynan masalani yechimi sifatida ishlatilib kelinmoqda. VPN zaifliklari albatda maxsus kanallarga xavf-xatarlarni keltirib chiqaradi. Ushbu maqolada aynan maxsus kanallarga bo‘ladigan xavf-xatarlarni aniqlash, baholash va boshqarish masalalari korib chiqilgan. Tahliliy natijalar asosida xavf-xatarlarni bartaraf etish uchun qo‘llashga bir necha yangi usullar taqdim etilgan.

Adabiyotlar tahlili va metodologiya. Ushbu maqolani yozishda bir qancha mavzuga oid adabiyotlar, ilmiy maqolalar o‘rganib chiqilgan. Ularni orasida tarmoq xavfsizlig protokollarini o‘rganishda R.X.Djurayev, SH.YU. Djabbarov, B.M.Umirzakovlarning “Tarmoq protokollari”[1] nomli o‘quv qo‘llanmasidan foydalanilgan, davlatlararo munosabatlar o‘rnatishda raqamli texnologiyalardan foydalanish yuzasidan M.S.Yakubov, F.M.Muxtarovlarning “Цифровая Дипломатия-приоритетный фактор формирования межгосударственных отношений”[2] maqolasi, axborot tizimlariga tahdidlarni tadqiq qilishda F.Muxtorov, A.Umarov, A.Ro‘zaliyevlarning “Axborot tizimlarida xavfsizlik tahdidlarining tasnifi”[3] va D.Tojimatov, J.Mirzayevlarning “Use of Artificial Intelligence Opportunities for Early Detection of Threats to Information Systems”[4] maqolalari, xavf-xatarlarni aniqlash, baholash va boshqarishni tashkil qilishda F.Muxtarovning “Axborot xavfsizligi xavflarini tahlil qilish uchun

https://doi.org/10.5281/zenodo.7978849

https://journals.indexcopernicus.com/search/article?articleId=3607082

https://al-fargoniy.uz/

ierarxik aktivlarni baholash usuli”[6] maqolasi tarmoq xatoliklari haqida ma’lumot olishda Kamolovich B. E. “Tarmoqlarda uzatiladigan ma’lumotlarni xatoliklarini bartaraf etish usullari”[7] maqolasi o‘rganilib, ulardan iqtiboslar keltirilgan.

Natijalar. Xar 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 mahsus 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.

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 xatolari xisoblanadi[4].

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 ob’ektiv (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[4].

Tahdid tushunchasi. Ma’lumki tahdidlar tabiiy va sun’iy turlarga bo‘linadi. Axborot xavfsizligi sohasida tahdidlarni o‘rganish juda muhum hisoblanib, mahsus 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[4].

Bir qarashda mahsus kanallar o‘zi himoya qatlamlariga ega bo‘lgan tarmoq deb tushuniladi. Aslida ham shunday. Katta tarmoqda alohida mahsus kanallar hosil qilish, ma’lumotlarni kriptografik vositalar yordamida shifrlash, kirishlarda atentifikatsiya usullarini qo‘llash, antivirus dasturlari, doimiy nazorat kabi barcha usullar mahsus kanalning muhim elementlari hisoblanadi. Lekin xech qanday to‘liq himoya tizimi mavjud bo‘lmagandek mahsus kanallar ham to‘lig‘ligicha xavf-xatarlardan holi emas. Ushbu dissertatsiyani asosiy mazmuni ham aynan o‘zining himoya usullariga ega mahsus kanallarga bo‘ladigan xavf-xatarlarni aniqlash va ularni bartaraf etishni nazarda tutadi. Mahsu kanallarga quyidagi zaiflik va tahdidlarni misol qilib keltirishimiz mumkun.

1. Fizik uzulishlar yoki barqarorlikdagi zaiflik. Bunda har qanday kanal qurishda kabel yoki radio-aloqadan foydalanamiz. Bu narsalar eskirishi, uzilishi, xatoliklar keltirib chiqarishi kabi zaifliklar ehtimoli mavjud. Bu o‘z navbatida kanallning barqaror ishlashini buzilishi tahdidini keltirib chiqaradi[3].

2. Mantiqiy xatoliklar. Bunda asosan qurilmalarning dasturiy ta’minotidagi buyruq xatoliklari, protokollarni tushunmaslik, dastur yangilanishlari qurilma konfuguratsiyasiga mos kelmasli, shifrlash usullarini kriptotahlilga uchrashi

https://doi.org/10.5281/zenodo.7978849

kabi zaifliklar. Ular esa ma’lumotlar buzilishi, shifrlashda xatolik, ma’lumotarni qayta deshifrlanmasligi, kontrol dasturlari tomonidan bloklanishi kabi tahdidlarni yuzaga chiqaradi[3].

3. Kadrlar muammosi. Sinalmagan yoki kimdir tomonidan josuslikka yollangan hodimlarga tarmoqni ishonib topshirish. Bu esa o‘z navbatida ma’lumotlarni qayta yo‘naltirish, tarmoqqa xost qo‘shish, ximoya tizimlarini o‘chirilishi kabi tahdidlarni yuzaga chiqaradi[3].

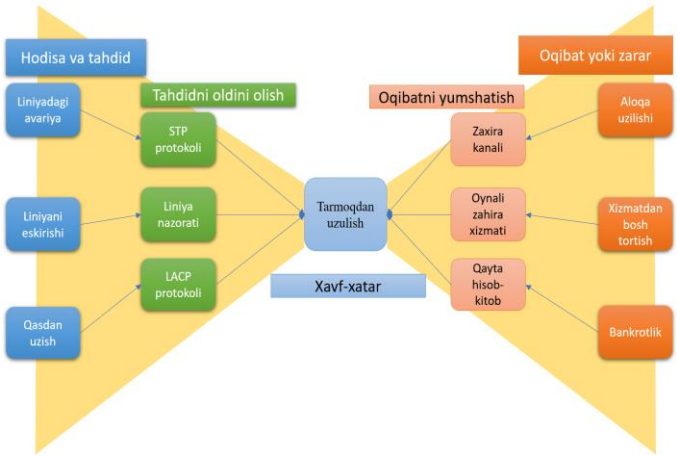
4. Texnologik muammo. Mahsus kanal qurishda foydalaniladigan mahsus qurulmalar firewallar, marshrutizatorlar, kommutatorlar, aloqa kabellarni bir-birining standartlariga mos kelmasligi yoki ishlab chiqaruvchisi tomonidan qandaydir ma’lumotlarni qo‘ga kiritishda yo‘lak qoldirib ketishi tahdidi xam yo‘q emas[3].

Mahsus kanallarga bo‘ladigan bunday tahdidlar va ular keltirib chiqishi mumkun bo‘lgan xavf-xatarlarni aniqlash va bartaraf etish uchun birinchi navbatda xavf-xatarni baholash va boshqarish talab etiladi. Keyingi bo‘limda biz albatta bu jarayonlarni qanday amalga oshirish kerakligi haqida ma‘lumot berib o‘tgan holda, xavf-xatarlarni baxolash usullari orqali ularni baholab chiqamiz.

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[5].

Risklarni baholash bosqichida tashkilotdagi risklarga baho beriladi va bu risklarning ta’siri yoki yuzaga kelish ehtimoli hisoblanadi. Risklarni baholash - uzluksiz davom etuvchi jarayon riskka qarshi kurashish rejalarini amalga oshirish uchun imtiyozlarni belgilaydi. Risklarni baholash ularning miqdoriy va sifatiy qiymatini aniqlaydi. Har bir tashkilot risklarni aniqlash, daraj alarga ajratish va yo‘q qilish uchun o‘zining riskni baholash jarayonini qabul qilishi kerak. Risklarni baholashda statik va analik usullar mavjud bo‘lib, ularni hodisalar daraxti usuli, galustik-babochka usuli, emprimik usul, anologdan foydalanish usuli, foyda-xarajat tahlili usuli, sezgirlik tahlili[5] kabi usullarni misol keltirishimiz mumkun.

Bizni holatda risklarni tahlil qilishda galustik babochka usuli yordamida baholashimiz mumkun. Agar maxsus kanalni tabiiy yoki sun’iy tahdidlar natijasida tarmoqdan uzilib qolishini xisobga olsak asosiy xavf-xatarni “Tarmoqdan uzilish” sifatida ko‘rishimiz mumkun. Agar tarmoqda uzilish xavf-xatari vujudga kelsa qabul qiluvchi va jo‘natuvchi tomonlar o‘rtasida “aloqada uzulishi”, korxona tashkilotlarning mijozlarini tarmoq orqali xizmat qabul qilolmasligi tufayli “xizmatdan bosh tortish”, asosiy hamkorlarni yo‘qotish natijasida “bankrotlik” kabi salbiy oqibatlarni yuzaga chiqarishi mumkun. 1-rasmda “Tarmoqdan uzilish” tahdidi mavjud bo‘lganda, tahdid xavf-xatarga yetguncha ularni bartaraf etish usullari, xavf-xatar amalga oshganda esa oqibatni yumshatish bo‘yicha usullar tahlili keltirib o‘tilgan. Natijada esa maxsus kanalni barqaror ishlashini ta’minlashga erishilishi mumkun.



1-rasm. Xavf-xatarlarni tahlil qilishda “Tarmoqdan uzilish” riskini Galstuk-babochka usuli yordamida baholash.

Muhokama. Demak oldin aytilganidek mahsus kanallarda ham zaifliklar mavjud, zaifliklar tahdidni keltirib chiqqaradi, tahdid esa xavf-xatarni, xavf-xatar zararli oqibatni. Bu zanjir to xavf-xatarga yetguncha biz xavflarni oldini olish usullarini ishlab chiqishimiz, bu usullar hujumlarga bardosh bermagan holda oqibatni yani zararni yumshatish usullarini ishlab chiqishimiz zarur ekan. Kompyuter tarmoqlarida mahsus kanal qurish VPN texnologiyasi (IPSec, L2TP protokollari, Xeshlash) usullari yordamida amalga oshirishini hisobga olsak. Yuqorida keltirib o‘tilgan hamda o‘rganilgan tahlillar asosida magisterlik dissertatsiyasini asosi sifatida quyidagi qo‘shimcha va yangi usullarni VPN bilan birgalikda foydalanishni tavsiya etaman.

1. **Tabiiy xavf-xatarlar uchun:**

- Mahsus kanlda STP protokolini qo‘llagan holda zaxira kanallarini hosil qilish[1]. Bunda tabiiy

https://doi.org/10.5281/zenodo.7978849

https://journals.indexcopernicus.com/search/article?articleId=3607082

hodisalar tufayli tarmoq kanallarida uzulish bo‘lganda avtomatik ravishda zaxira kanalidan foydalanish ta’minlanadi;

- LACP protokoli yordamida kanalni agregatlash[1]. Bunda mahsus kanalda axborot oqimini sekinlashish hodisasi oldi olinib, kanaldagi axborot tez almashinishi ta’minlanadi.

2. Sun’iy xavf-xatarlar uchun:

- Autentifikatsiya uchun AAA (authentifikation, authorization, accounting) usulini Radius serverida qo‘llash. Bunda korxonaninghar bir hodimi uchun avtorizatsiyadan o‘tishda alohida identifikator va autentifikator berilishi nazarda tutiladi. Biror xavf-xatar sodir bo‘lganda aynan qaysi hodimni login, paroli yordamida hodisa sodir bo‘lganini aniqlash imkoniyati mavjud bo‘ladi.
- SNMP (Simple Network Management Protocol) protokoli yordamida barcha hodisalarni log fayllarini ichki serverga qayt etib borish[1]. Bunda xavf-xatarlarni tahlil qilish tarmoq administratorlariga qulaylik yaratadi.
- DHCP SNOOPING xavfsizlik sozlamalarini o‘rnatish. Bunda korxonani ichki tarmoqlaridagi qurilmalar buzg‘unchi tomonidan sohta ip manzillar berilishi xavf-xatari oldi olinadi.
- ARP spoofingga qarshi anti ARP spoofing va ARP anti-flood xizmatlarini o‘rnatish. Bunda buzg‘unchi tomonidan kanalda yuboriladigan sohta so‘rovlar (DDOS hujumi) natijasida qurilmalarni kanalda axborot oqimini toshishi hodisasi oldi olinadi.
- ASA xavfsizlik devorini (firewall) o‘rnatish. Bunda mahsus kanalga bo‘ladigan tashqi va ichki tahdidlar oldi olinadi. Mahsus kanallarda axborotlarni kirishi va chiqishiga nazorat o‘rnatiladi.

Xulosa. Xulosa qilib aytganda maxsus axborot almashuv kanallari ham xavf-xatarlarga qarshi yuqori darajadagi himoyani ta’minlay olmaydi. Maqolada takidlab o‘tilganidek xar qanday xavfsizlik tizimlarining o‘ziga yarasha zaiflik tomonlari mavjud bo‘ladi. Axborot xavfsizligi mutaxassisi xavf-xatarlarga qarshi chora-tadbirlar ishlab chiqishda birinchi navbattda xavf-xatarni aniqlash va uni to‘g‘ri baholay olishi zarur. Agar yuzaga kelishi mumkun bo‘lgan xavf-xatarlarni to‘g‘ri tahlil qilinishiga erishilsa, ularni bartaraf etish usullarini ham qo‘llay oladi. Ushbu maqolada maxsus kanallarda asosan tabiiy yoki sun’iy tahdidlar tufayli yuzaga kelishi mumkun bo‘lgan “Tarmoqdan uzilish” xavfi tahlil qilinib, baholash usuli keltirib o‘tilgan. Xavf-xatarni baholashdan olingan natijaga ko‘ra tarmoq xavfsizligi protokollari va texnologiyalarini ketma-ketlikda qo‘llash bo‘yicha yangi usul taklif etilgan.

Taklif etiladigan usullarni mahsus kanallarga qo‘llash korxona xarajati o‘sishiga salbiy ta’sir ko‘rsatmaydi. Ammo usullarni qo‘llash va doimiy nazorat qilish uchun alohida xavfsizlik mutaxassisi jalb qilinishi maqsadga muofiq sanaladi.

Ushbu maqola materiallaridan mavzu mazmuni bo‘yicha ilmiy izlanuvchilari o‘z ilmiy ishlarida iqtibos keltirgan holda foydalanishlari mumkun.

ADABIYOTLAR RO‘YXATI

[1]. R.X. DJURAYEV, SH.YU. DJABBAROV, B.M. UMIRZAKOV “TARMOQ PROTOKOLLARI”, o‘quv qo‘llanma, Toshkent-2018.

[2]. M.S.Yakubov, F.M.Muxtarov., “ЦИФРОВАЯ ДИПЛОМАТИЯ-ПРИОРИТЕТНЫЙ ФАКТОР ФОРМИРОВАНИЯ МЕЖГОСУДАРСТВЕННЫХ ОТНОШЕНИЙ”., НАУЧНЫЕ РАЗРАБОТКИ: ЕВРАЗИЙСКИЙ РЕГИОН 2017,.

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

[4]. 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.

[5]. 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.

[6]. Muxtorov F. M. et al. AXBOROT XAVFSIZLIGI XAVFLARINI TAHLIL QILISH UCHUN IERARXIK AKTIVLARNI BAHOLASH USULI //INTERNATIONAL CONFERENCES. – 2022. – Т. 1. – №. 4. – С. 76-80.

[7]. Kamolovich B. E. TARMOQLARDA UZATILADIGAN MA’LUMOTLARNI XATOLIKLARINI BARTARAF ETISH USULLARI //Scientific Impulse. – 2022. – Т. 1. – №. 4. – С. 1637-1640.

https://doi.org/10.5281/zenodo.7978849

https://journals.indexcopernicus.com/search/article?articleId=3607082