# AXBOROTLASHTIRISH RESURSLARI VA OBYEKTLARINING KIBERXAVFSIZGINI TA’MINLASHDA SINOV LABORATORIYALARINING AHAMIYATI

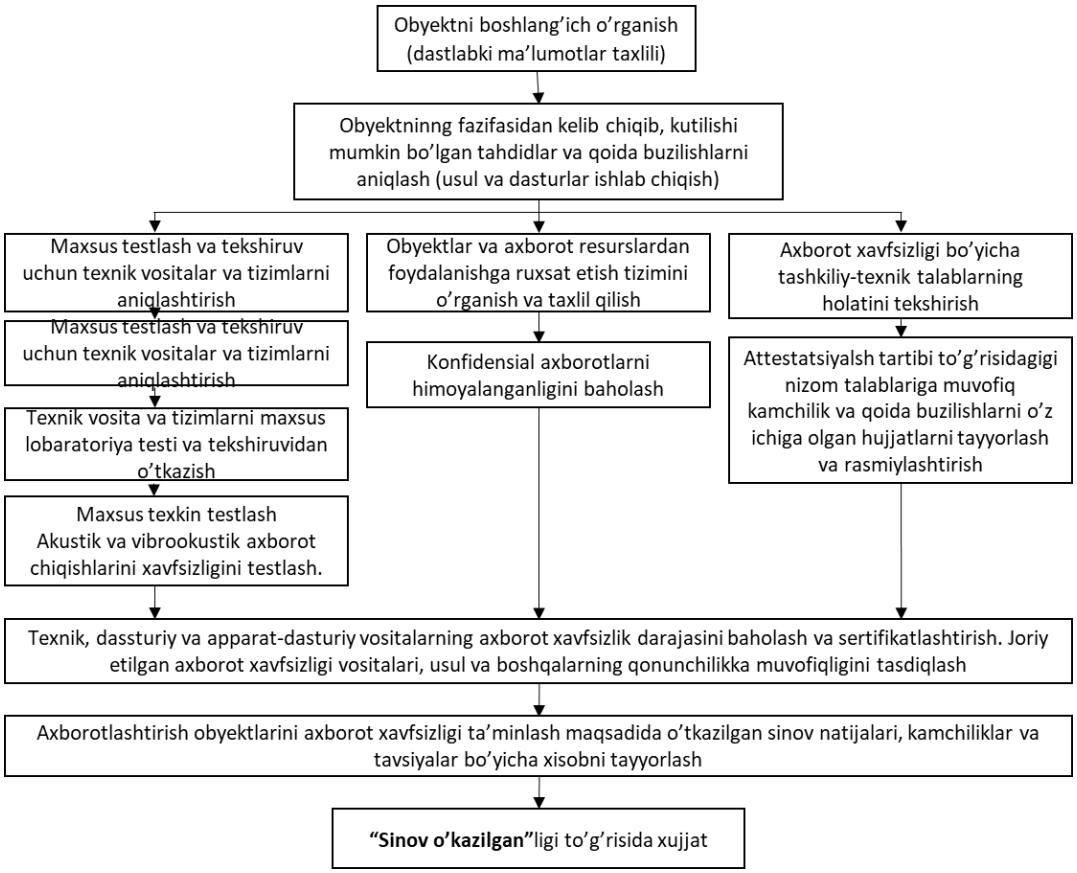
**Meliko‘ziev R.Sh**
**Radjabova M.Sh**
**Qurbonmurodov D.U**
*Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti, O’zbekiston, Toshkent*

**Annotatsiya:** *Mazkur maqola axborotlashtirish obyektlari va axborot resurslari axborot xavfsizligi bo’yicha darajasini aniqlashni amalga oshiruvchi sinov laboratoriyasi to’g’risida. Shuningdek maqolada sinov laboratoriyasining kiberxavfsiz darajasini baholash bo’yicha asosiy yo’nalishlari va tamoyillari hamda hozir kunda qo’llanilib kelinayotgan xavfsizni tekshiruvchi, testlovchi va tahlil qiluvchi dasturiy vositalarning turlari to’g’risida ma’lumotlar beriladi.*

**Kalit so’zlar***: Axborotlashtirish obyektlari, axborot resurslari, axborot xavfsizligi, axborot tahdidlari, kiber hujum, sinov laboratoriyasi, , tekshirish, ruxsatsiz kirish, testlash, tahlil sinovlari, baholash.*

## KIRISH

Kundan kunga axborot texnologiyalari rivojlanmoqda. Har daqiqada yangi dastur va qurilmalar ishlab chiqilmoq. Ishlab chiqaruvchilarning barchasi ham uning xavfsizlik jihatlariga e’tibor qaratayotgani yoq. Axborot resurslarining xavfsizlik bo’yicha baholash uning hayotga joriy etilishini belgilab beruvchi faktor hisoblanadi[1]. Xavfsizlik darajasi baholash uchun albatta yuqori malakali dasturchi mutaxassislar va zamonaviy testlash dasturiy va apparat-dasturiy vositalari kerak bo’ladi. Agar ularni umumlashtiradigan bo’lsak, umumiy qilib sinov laboratoriya tashkil etish mumkin. Mazkur sinov laboratoriyalari kiberxavfsizlik, axborotni kiber hujumlardan muhofaza qilish va raqamli kriminalistika, tarmoq ma’lumotlarini boshqarish, maxfiy ish yuritish bo‘yicha amaliy mashg‘ulotlar hamda sinov-tajribalarini o‘tkazish, tadqiqotlar va axborot-tahliliy faoliyat olib borishi mumkin. Axborotlashtirish obyektlarini sinovlarini o'tkazishning umumlashtirilgan sxemasi 1-rasmdagi sxemada ko’rsatilgan.




1 rasm. Axborotlashtirish obyektlarini attestatsiya sinovlaridan o'tkazishning umumiy sxemasi.

## SINOV LABORATORIYASINING KIBERXAVFSIZ DARAJASINI BAHOLASH BO’YICHA ASOSIY TAMOYILLARI

Axborotlashtirish resurslari va obyektlarining kiberxavfsiz darajasini baholab beruvchi sinov laboratoriyalarining asosiy maqsadi quyidagilardan iborat bo’lishi talab etladi[2,5]:

•kiberxavfsizlika va kriminalistika bo‘yicha o‘quv-uslubiy, sinov-laboratoriya va amaliy mashg‘ulotlarni o‘tkazish;

•ekspertlarni laboratoriyaga jalb etish. kiberxavfsizlik va kriminalistika sohasida yuqori malakaga ega bo‘lgan va amaliy tajribaga ega mutaxassislarni laboratoriya faoliyatiga jalb etish;

•ilmiy va innovatsion loyihalarni amalga oshirish. ichki va tashqi ilmiy loyihalarni olish va amalga oshirish;

•universitetining ilmiy salohiyatini oshirish. ilmiy loyihalarni amalga oshirish orqali yangi ilmiy-amaliy yangiliklar ishlab chiqish va bu orqali mamlakatimizda ijtimoy va iqtisodiy samaradorlikka erishish;

•kiberxavfsizlik va kriminalistika bo‘yicha (axborot texnologiyalariga doir) davlat hamda boshqa buyurtmalarini bajarish;

•axborotlashtirish obyektlarini attestatiyadan o‘tkazish va axborot reserslarini axborot xavfsizligi bo‘yicha sug‘urtalash tizimini rivojlantirish;

## SINOV LABORATORIYALARINING ASOSIY YO‘NALISHLARI

Sinov laboratoriyalarining 6 ta ustivor faoliyat yo’nalishidan iborat bo’lishi mumkin:

1. “Murakkab tizimlarda axborot xavfsizligi jarayonlarini modellashtirish” ixtisoslashtirilgan xona axborotni muhofaza qilish va axborot xavfsizligi sohasida amaliy ko‘nikmalarni egallash uchun mo‘ljallangan. Auditoriya zamonaviy hisoblash va ixtisoslashtirilgan uskunalar bilan jihozlangan 20 ta avtomatlashtirilgan o‘quv o‘rni, shuningdek, obyektlarda axborot xavfsizligi tizimlarini tashkil etish va axborot xavfsizligi auditi bo‘yicha laboratoriya va amaliy ishlarni oshirish imkonini beruvchi litsenziyalangan dasturiy ta’minot bilan jihozlanadi[12]. Har qanday murakkablikgagi kompyuter tarmoqlarida axborot xavfsizligi tizimlarini yaratishda VipNet va SecretNet dasturiy-apparat tizimlari, shuningdek, GRIF 2.0 axborot risklarini tahlil qilish va boshqarish tizimi, CONDOR 3.0 axborot xavfsizligi siyosatini ishlab chiqish va boshqarish tizimi kabi boshqa maxsus dasturlardan foydalaniladi.

2. "Elektron hujjat aylanishi va maxfiy ish yuritish" ixtisoslashtirilgan xona korxonada maxfiy ma'lumotlar (tijorat siri, kasbiy sirlar, shaxsiy ma'lumotlar) muhofazasini boshqarish va tashkil etishni hujjatli ta'minlash jarayonida eng yangi kompyuter axborot texnologiyalarini joriy etish va ulardan foydalanish bo‘yicha mashg‘ulotlar o‘tkazish uchun mo‘ljallangan. Mashg‘ulotlar eng yirik dasturiy ta’minot kompaniyalari tomonidan yetkazib beriladigan “Delo”, “Kadrlar”, “Letograf”, “Boss-referent”, “Lotus Notes Domino” va hokazo elektron hujjat aylanish tizimlaridan foydalangan holda zamonaviy uskunalarda o‘tkaziladi. Uskuna va dasturiy ta'minot zamonaviy elektron ofisda axborotni qabul qilish va uzatishning barcha usullaridan foydalangan holda real rejimda biznes o‘yinlarini tashkil qilish va o‘tkazish imkonini beradi.

3. “Hududiy boshqaruvni axborot-tahliliy qo‘llab-quvvatlash” ixtisoslashtirilgan xona avtomatlashtirilgan axborot-tahlil tizimidan foydalangan holda davlat boshqaruvi va biznesda boshqaruv qarorlarini qabul qilishni qo‘llab-quvvatlash maqsadida axborotni to‘plash, tahlil qilish va tahliliy qayta ishlash bo‘yicha mashg‘ulotlar o‘tkazish uchun mo‘ljallanadi. Xonani jihozlashda android o‘quv dasturlari yordamida o‘rganish mashg‘ulotlari olib boriladi.

4. "Psixo-fiziologik va ijtimoiy ta'minot" ixtisoslashtirilgan xona psixofiziologik xavfsizlikni o‘qitish usullari va ijtimoiy xavfsizlikni ta'minlash texnologiyalari bo‘yicha mashg‘ulotlar o‘tkazish uchun mo‘ljallangan. Sinfda funktsional holatni o‘z-o‘zini tartibga solish bo‘yicha psixo-treninglar, mijozlar bilan ishlash bo‘yicha treninglar o‘tkaziladi. Favqulodda vaziyatlarda shoshilinch axborot xavfsizligini ta’minlash bo‘yicha amaliy mashg‘ulotlar olib boriladi. Shuningdek Xakerlar psixologiyasi va uning asosiy yondashuv yo‘nalishlari taqlid qilish shaklida o‘rganiladi va unga qarshi usullar tahlil qilinadi. "Maks" elektron majmuasi, shuningdek, ko‘rgazmali materiallar va o‘quv dasturlari yordamida amalga oshiriladi.

5. "Himoya qilinadigan binolarning axborot xavfsizligini boshqarish tizimi" ixtisoslashtirilgan xona maxfiy ma'lumotlar bilan ishlash uchun sertifikatlangan xavfsiz xonani tashkil etish va undagi maxfiy uchrashuvlarning axborot xafsizligini ta’minlash bo‘yicha tashkiliy va texnik chora-tadbirlarni amalga oshirish usullari tadqiq qilinadi[4,9].

6. Penetratsion testlar mavjud zaifliklar va ulardan foydalanish oqibatlari haqida ma'lumot olish, mavjud himoya choralari samaradorligini baholash va aniqlangan muammolarni bartaraf etish va xavfsizlik darajasini oshirish bo‘yicha keyingi harakatlar (tavsiyalar)ni rejalashtirish imkonini beradi. Penetratsion test tashkilotlardan PCI DSS kabi tizim xavfsizligini muntazam tekshirib turish, hamda talab qilinadigan xavfsizlik standartlariga muvofiqligini tahlil qilish mumkin.

## PENETRATSION TESTLARNING TURI

Penetratsion testlar:

- Tashqi kirish testi. Tashkilotning IT infratuzilmasi bo‘yicha dastlabki ma'lumotlarsiz tashqaridan amalga oshiriladi.
- Ichki kirish testi. Ofisga faqat jismoniy kirish huquqiga ega bo‘lgan tashrifchi yoki muayyan tizimlarga cheklangan kirish huquqiga ega bo‘lgan pudratchi kabi ichki tajovuzkorning harakatlari simulyatsiya qilinadi.

Ijtimoiy muhandislik usullaridan foydalangan holda sinovlar Fishing, zararli elektron pochta havolalari, shubhali qo‘shimchalar va boshqalar kabi ijtimoiy muhandislik hujumlarini taqlid qilish orqali xodimlaringizning axborot xavfsizligi bo‘yicha xabardorligini baholashga qaratiladi[12].

Simsiz tarmoq xavfsizligi tahlili. Wi-Fi tarmoqlarining xavfsizlik darajasini baholash.

Ilovalar xavfsizligini tahlil qilish ilovalarni himoya qilishda turli aniqlash va xavfsizlik muammolarini zudlik bilan bartaraf etish, hamda kiberhujumlar natijasida yuzaga kelishi mumkin bo‘lgan moliyaviy va obro‘ga zarar yetishi oldini olish. Laboratoriyada tajribaga ega bo‘gan mutaxassislar tomonidan har xil turdagi ilovalar, jumladan, veb-ilovalar, mobil ilovalar, korporativ portallar, masofaviy bank tizimlari va boshqalar xavfsizligi tahlil qilinadi. Zaifliklarni aniqlashning asosiy yondashuvi sifatida ekspert va na’munaviy dastur sinovdan o‘tkaziladi. Bu hatto eng murakkab muammolarni, shu jumladan ilovaning biznes imkoniyatlarini oshirish bilan bog‘liq muammolarni aniqlashga yordam beradi.

## VEB ILOVALARNING XAVFSIZLIK DARAJALARINI BAHOLASH

Ilovalar xavfsizligini tahlil qilish:

- qora quti sinovi. tashqi tajovuzkorning harakatlarini taqlid qilish;
- kulrang quti sinovi. turli imtiyozlarga ega bo‘lgan ro‘yxatdan o‘tgan foydalanuvchilar tomonidan hujumning simulyatsiyasi;
- oq quti sinovi. ilovaga, shu jumladan manba kodiga to‘liq kirish imkoniyati bilan tahlil qilish
- ilovaga hujumlarni aniqlash, tizimining samaradorligini tahlil qilish. hujumlarni aniqlash va blokirovka qilish, WAF qo‘llanilganligi va uning samaradorligini tekshirish.

Bankomatlar va POS-terminallar xavfsizligini kompleks tahlil qilish tajovuzkorlar tomonidan naqd pul yechib olish, ruxsat etilmagan operatsiyalarni amalga oshirish, mijozlaringizdan to‘lov kartalari ma’lumotlarini yig‘ish yoki DoS amalga oshirish maqsadidagi hujumlarni tahlil qilish. Bankomatlar va POS-terminallarni himoya qilish tizimidagi zaifliklarni aniqlash, shuningdek, ularning ishlashining mumkin bo‘lgan oqibatlarini baholash va joriy etilgan himoya choralari samaradorligini aniqlash, hamda xavfsizlik darajasini oshirish, shuningdek, aniqlangan muammolarni bartaraf etish bo‘yicha zarur harakatlar to‘g‘risida ma'lumot olish imkonini beradi[3,9].

## TERMINAL VA BANKOMATLARNING KIBERXAVFSIZLIGINI TEKSHIRISH

Bankomatlar va POS-terminallar xavfsizligini kompleks tahlil qilish 4 bosqichda amalga oshiriladi:

1. Zaiflikni aniqlash. Dasturiy ta'minotning eskirgan versiyalarida konfiguratsiya kamchiliklari va zaifliklarini aniqlash.
2. Mantiqiy tahlil. Komponentlar darajasida yangi zaifliklarni aniqlash uchun bankomatlaringiz va POS-terminallaringiz tomonidan bajariladigan jarayonlarning mantiqiy tahlili.
3. Hujum simulyatsiyasi. Himoyalanish samaradorligini amalda baholash uchun haqiqiy hujumni simulyatsiya qilish.
4. Kompleks hisobot. Barcha aniqlangan zaifliklar va xavfsizlik kamchiliklarining batafsil tavsifi, ularni darhol bartaraf etish bo‘yicha amaliy tavsiyalar.

Sanoat tizimlarining xavfsizligini tahlil qilish korxonaga xos tahdidlarni modellashtirish va sanoat jarayonlarini boshqarish tizimlarida zaifligini tahlil qilish, hujumlarning potentsial ko‘rsatkichlari hamda hujumlarning texnologik va biznes jarayonlarga ta'sirini baholanishi mumkin.

Laboratoriya sanoat tizimlari xavfsizligini tahlil qilish, jismoniy va tarmoqda barcha darajadagi ICS himoyasidagi zaif tomonlarni aniqlash imkonini beradi . Ma'lumotlarni yig‘ish va nazorat vositalrini nazorat qilish SCADA tizimlari va PLC kontrollerlari tahlil qilinadi[10]. Zaifliklardan foydalanishning mumkin bo‘lgan oqibatlari haqida ma'lumot o‘rganiladi va qo‘llaniladigan himoya choralari samaradorligi baholanadi, bu aniqlangan muammolarni bartaraf etish va xavfsizlik darajasini oshirish bo‘yicha keyingi harakatlarni rejalashtirish imkonini beradi.

## SANOAT TIZIMLARINING XAVFSIZLIGINI TAHLIL QILISH

Sanoat tizimlarining xavfsizligini tahlil qilish yo’nalishlari quyidagilardan iborat:

1. Penetratsiya testi mavzud turli toifadagi tajovuzkorlarning harakatlariga taqlid qilish, uning maqsadi mavjud imtiyozlarni kengaytirish va jarayonni boshqarishning avtomatlashtirilgan tizimiga ruxsatsiz kirishdir.
2. ICS infratuzilmasi xavfsizligini tahlil qilish. Oq quti usuli yordamida amalga oshiriladi va jarayonni boshqarish tizimlari uchun texnik hujjatlarni tahlil qilish, xodimlar bilan muloqatlar, sanoat tizimlari va ishlatiladigan protokollarni tahlil qilish, shuningdek,

sanoat ekspluatatsiyasi jarayonida jarayonni boshqarish tizimining tarkibiy qismlarining texnologik auditini o‘z ichiga oladi.

3. ICS komponentlarini xavfsizlik tahlili. Yangi zaifliklarni aniqlash maqsadida jarayonni avtomatlashtirilgan boshqarish tizimining dasturiy va apparat-dasturiy komponentlarining xavfsizligini sinov muhitida chuqur o‘rganish, shundan so‘ng real tizimda aniqlangan zaifliklar mavjudligini qo‘shimcha tekshirish amalga oshirilishi mumkin[11].

4. Kompleks hisobot. Barcha aniqlangan zaifliklar va xavfsizlik kamchiliklarini tavsiflovchi, ularni darhol bartaraf etish bo‘yicha amaliy tavsiyalarni o‘z ichiga olgan xulosa hisoboti.

5. "Aqlli" texnologiyalar va IoT xavfsizligini tahlil qilish zamonaviy yuqori darajada integratsiyalangan qurilmalar va ularning o‘ziga xos infratuzilmalari xavfsizligini batafsil va har tomonlama baholash, proshivka, ilova va tarmoqlarning o‘zaro ta'siri darajasidagi zaifliklarni aniqlash va tahlil qilish.

**"Aqlli" texnologiyalar va IoT xavfsizligini tahlil qilish** zamonaviy yuqori darajada integratsiyalangan qurilmalar va ularning o'ziga xos infratuzilmalari xavfsizligini batafsil va har tomonlama baholash, proshivka, ilova va tarmoqlarning o'zaro ta'siri darajasidagi zaifliklarni aniqlash va tahlil qilish.

“Aqlli” texnologiyalar va IoT xavfsizligini tahlil qilish:

a. O'rnatilgan qurilmalarning xavfsizligini tahlil qilish. Platformaning normal ishlashini buzish uchun tajovuzkorlar tomonidan ishlatilishi mumkin bo'lgan zaifliklarni, dizayn xatolarini va konfiguratsiya muammolarini aniqlash uchun o'rnatilgan qurilmalarning apparat va dasturiy ta'minot qismlarining xavfsizlik darajasini baholash.

b. Ilova xavfsizligi tahlili. O'rnatilgan tizimlarning ishlashini kuzatish va boshqarish uchun foydalaniladigan ilovalar xavfsizligini chuqur tahlil qilish, shu jumladan manba kodi va dastur arxitekturasini statik va dinamik tahlil qilish.

c. Penetratsiya testi. Mavjud himoyalarni chetlab o'tishga va turli xil tajovuzkor modellari nuqtai nazaridan muhim tizimlarni buzishga qaratilgan o'rnatilgan qurilmalarning ishlashini ta'minlaydigan AT infratuzilmasini tahlil qilish.

d. Batafsil hisobotlar. Barcha aniqlangan zaifliklar va xavfsizlik muammolari va ularni tezda bartaraf etish bo'yicha amaliy tavsiyalar tavsiflangan umumiy hisobot[2,12].

**Red Team bilan sinov** monitoring qobiliyati va hodisalarga javob berish tartib-qoidalarining samaradorligini baholash uchun tahdid razvedkasiga asoslangan hujum simulyatsiyasilarini o’rganish.

**Hakerlik sohasini tadqiq iqlish,** ular foydalanadigan dastur va usullarni tahlil qilish, kiber hujumlarni amalga oshirgan hakerlar to’g’risidagi ma’lumotlarni aniqlash, hujumning maqsadi, hujim natijalari va keltirilgan zararni baholash.

**Xotira qurilmalarini tahlil qilish.** Sindirilgan apparat-dasturiy vositalarning xotira qurilmalarini tiklash, udan malumotlarni olish va tahlil qilish.

**Tarmoqqa ulanish usullarini tahlil qilish.** Xavfsizligi taminlangan apparat dasturiy qurilmalarga va tarmoqqa fizik ulanish orqali ma’lumotlarni olish, shifrlangan

ma’lumotlarni ochish, kriptobardoshligini baholash, kalitlar generatsiyasi va ularga ta’sir o’tkazish. Mavjud kamchiliklarni bartaraf etish va xavfsizlikni ta’minlash bo’yicha chora-tadbirlarni ishlab chiqish.

**Apparat-dasturiy qurilmalaridan ruxsatsiz foydalanishni tahlil qilish.** Operatsion tizimlarga ruxsatsiz kirish, ma’lumotlarni olish, ularga o’zgartirish kiritish va uning natijalari, o’zgartirishlarni tiklash, zararni baholash, xakerlar tomonidan qilingan ishlar va jarayonlarni tahlil qilish.

## XULOSA

Taklif etilayotgan na’munaviy kiberxavfsizlik va kreminalistika sinov laboratoriyaning asosiy vazifa va maqsadini umumashrirgan holda barcha texnik jihozlar va vositalarni bir xonada yoki mobil majmuada mujassamlashtirish mumkin.

Sinov laboratoriyasi axborot xavfsizligini ta’minlashning asosiy choralaridan biri hisoblanib, olingan sinob natijalari asosida axborot resurslarini hayotga joriy etilishiga ruxsat berish maqsadga muvofiqdir. Raqamli texnologiyalar rivojlanishi jadallashmoqda, bu esa xakerlar hujumiga bardosh olish kabi muhim muammolarni keltirib chiqarmoqa. Hujumlar natijasida yuzaga kelgan talofatlarni bartaraf etish yoki qoplashni sinov o’tkazgan laboratoriya ham o’z javovgarligiga olmaydi. Lekin sinov o’tkazilishi natijasida axborot resursining kiber himoyalanganlik darajasi aniqlanadi. Olingan natijalar asosida kamchiliklar to’g’irlanishi uning himoyalangan ko’rsatkichi oshiradi. Xavfsizlikni doimiy ta’minlash maqsadida konponiyalar o’z axborot tizmini doimiy testlab boradi va hujumlarga qarshi ataka usulini amalga oshiradi. Shu orqali kutilishi mumkin bo’lgan talofatlarning oldini oladi.

## ADABIYOTLAR:

[1] O‘zbekiston Prezidentining farmoni 2022-2026 yillarga mo‘ljallangan yangi O‘zbekiston taraqqiyot strategiyasi 2022-yil.‘

[2] Qilichev.U.V Axborot texnologiyalari sohasida jinoiylarga qarshi kurash bo‘limi o‘ta katta ishlarni bajarish tezkor vakil, podpolkovnik. 23.12.2019.

[3] Scannell, Kara (24 February 2016). «CEO email scam costs companies $2bn». Financial Times (25 Feb 2016). Archived from the original on 23 June 2016. Retrieved 7 May 2016.

[4] «What is Spoofing? – Definition from Techopedia». Archived from the original on 30 June 2016.

[5] Marcel, Sébastien; Nixon, Mark; Li, Stan, eds. (2014). Handbook of Biometric Anti-Spoofing: Trusted Biometrics under Spoofing Attacks (PDF).London: Retrieved 8 October 2017.

[6] «Spoofing». Oxford Reference. Retrieved 8 October 2017.

[7] Fedotov N.N. DoSataki v Seti. Vvedenie, tekushchaya amaliyot i prognoz // «Dokumentalnaya elektrosvyaz» jurnali. 2015 yil. №13 http://www.rtcomm.ru/about/press/pa/?id=429.

[8] Nurmatov B. Qashqadaryo viloyat IIB xodimi. Kiberterrorizm shiddat bilan o‘sib borayotganiga sabab nima.17.03.2019.

[9] https://Qashqadaryo.uz/oz/nview/kiberterrorizm-shiddat-bilan-%D0%BE-sib-borayotganiga-sabab-nima-17-03.

[10] Полная статистика угроз информационной безопасности в одной статье.07.10.2021.https://codernet.ru/articles/drugoe/polnaya_statistika_ugroz_informaczionnoj_bezopasnosti_v_odnoj_state/

[11] Афтер Амир. Развитие информационных угроз в третьем квартале 2022 года. Статистика по ПК. 18 ноя 2022. https://securelist.ru/it-threat-evolution-in-q3-2022-non-mobile-statistics/106077/

[12] Кибератаки. 2023/01/17 https://www.tadviser.ru/index.php/