FAYL METAMA'LUMOTLARINI HIMOYALASHDA SUN'IY INTELLEKT ASOSIDA TAHDIDLARNI ANIQLASH VA JAVOB QAYTARISH ALGORITMLARI

Sodiqova Dilnoza Jumanazarovna

Muxammad al – Xorazmiy nomidagi TATU "Kiberxavfsizlik va kriminalistika" kafedrasi assistenti.

Email: sodiqovadilnoza655@gmail.com

Annotatsiya. Ushbu maqolada raqamli hujjatlar tarkibidagi metama'lumotlarni himoyalash bo'yicha sun'iy intellekt asosidagi tahdidlarni aniqlash va avtomatik javob qaytarish modeli ishlab chiqildi. Metama'lumotlar — muallif, yaratilish va tahrir vaqti, GPS koordinatalar, qurilma identifikatori, versiya tarixi kabi texnik atributlar — ko'pincha foydalanuvchi tomonidan nazorat qilinmaydi, biroq ular sezilarli xavfsizlik xatarlari manbai hisoblanadi. Tadqiqotda Autoencoder, LSTM, Isolation Forest kabi AI modellaridan foydalanilib, metadata anomaliyalarining yuqori aniqlikda aniqlanishi ta'minlandi. Shuningdek, AES-GCM, RSA-OAEP va SHA-3 algoritmlariga asoslangan selektiv kriptografik himoya modeli ishlab chiqilib, metadata qatlamining maxfiyligi va yaxlitligi oshirildi. Tarmoq darajasida TLS 1.3, DPI va IDS/IPS texnologiyalari yordamida tranzit jarayonidagi metadata sizishining oldi olindi. Natijalar taklif etilgan model raqamli hujjatlar xavfsizligi uchun kompleks, moslashuvchan va samarali yechim ekanligini ko'rsatdi.

Kalit so'zlar *metama'lumotlar, sun'iy intellekt, anomaliya aniqlash, kriptografik himoya, AES-GCM, RSA-OAEP, SHA-3, metadata forensikasi, hujjat xavfsizligi, TLS 1.3.*

Аннотация. В статье представлен усовершенствованный подход к защите метаданных цифровых файлов на основе искусственного интеллекта. Исследование охватывает анализ скрытых структур DOCX, PDF и EXIF-метаданных, а также выявление аномальных признаков, которые могут указывать на подмену, утечку конфиденциальной информации или несанкционированное редактирование. Для автоматического обнаружения угроз были применены модели Autoencoder, LSTM и XGBoost, обеспечившие высокую точность при определении отклонений в метаданных. Разработанный механизм реагирования использует гибкую криптографическую политику, предусматривающую выборочное шифрование чувствительных полей на основе AES-GCM и контроль целостности с помощью SHA-3. Дополнительно модель интегрирована с сетевыми механизмами защиты, включающими TLS 1.3 и интеллектуальную систему обнаружения вторжений. Результаты экспериментов подтверждают, что предложенный подход существенно снижает риск атак, связанных с

ISSN 3030-3907

метаданными, и может быть адаптирован для государственных, корпоративных и облачных систем.

Ключевые слова : защита метаданных, искусственный интеллект, XGBoost, LSTM-анализ, шифрование AES, контроль целостности, EXIF-угрозы, сетевые протоколы безопасности, IDS/IPS

Abstract. This study introduces a novel AI-driven framework for protecting metadata embedded within digital documents. The approach begins with extracting and profiling metadata fields from DOCX, PDF, and EXIF-based images to identify structural inconsistencies and security-critical attributes. Advanced machine learning models — including Autoencoder, BiLSTM, and XGBoost — were trained to detect anomalous metadata patterns associated with data leakage, unauthorized modification, or targeted cyberattacks. A selective protection strategy was implemented, applying AES-GCM encryption, SHA-3 integrity validation, and RSA-OAEP key handling only to metadata fields classified as high-risk. For secure transmission, the system integrates TLS 1.3 alongside an AI-enhanced intrusion detection module capable of intercepting hidden metadata leakage over the network. Experimental evaluation demonstrates that the proposed framework significantly strengthens metadata resilience and provides a scalable defense mechanism for modern e-government, enterprise security, digital forensics, and cloud environments.

Keywords: metadata protection, AI-based detection, BiLSTM, Autoencoder, XGBoost, selective encryption, AES-GCM, SHA-3 integrity, metadata leakage, TLS 1.3

Kirish.

Raqamli transformatsiya jarayoni jadal kechayotgan hozirgi davrda elektron hujjatlar, raqamli kontent va ularga biriktirilgan metama’lumotlar (metadata) global axborot ekotizimining ajralmas qismiga aylandi. Davlat boshqaruvi, bank tizimi, sog‘liqni saqlash, sud-ekspertiza, korporativ boshqaruv, masofaviy ta’lim va elektron tijoratda har kuni millionlab fayllar yaratilmoqda, qayta ishlanmoqda va almashilmoqda. Ushbu fayllardagi asosiy kontentdan tashqari, ularning ichki strukturasi — *metadata* — foydalanuvchi uchun sezilmas, ammo axborot xavfsizligi nuqtayi nazaridan nihoyatda muhim bo‘lgan ma’lumotlarni o‘z ichiga oladi.

Metama’lumotlar odatda faylning muallifi, yaratilgan vaqti, joylashuvi, dastur versiyasi, qurilma identifikatori, o‘zgartirish tarixi, EXIF GPS koordinatalari, versiya ketma-ketligi, yashirin matnlar, hujjat shabloni, tarmoq izlari yoki boshqa texnik atributlarni o‘z ichiga oladi. Ular dastlab hujjatni boshqarish va texnik kuzatuvni qulaylashtirish uchun yaratilgan bo‘lsa-da, kiberjinoyatchilar tomonidan ekspluatatsiya qilinganda sezilarli darajada xavf

ISSN 3030-3907

tug‘diradi. So‘nggi tadqiqotlar metadata orqali shaxsni aniqlash (identity leakage), geo-lokatsiyani aniqlash, tashkilot ichki tuzilmasini modellashtirish, spear-phishing hujumlari uchun profil yaratish, xodimlar faoliyatini kuzatish va maxfiy jarayonlarni tiklash mumkinligini ko‘rsatmoqda.

An’anaviy axborot xavfsizligi vositalari — antiviruslar, IDS/IPS tizimlari, trafik filtrlari, firewalllar — odatda kontentga yo‘naltirilgan bo‘lib, metama’lumotlarni alohida xavf sifatida ko‘rmaydi. MAT2, ExifCleaner yoki boshqa metadata tozalash utilitalari esa faqat qo‘lda ishlaydi va har doim ham metadata to‘liq aniqlanmaydi, ba’zi atributlar esa tozalanganda hujjatning funksionalligini buzadi. Natijada, metadata orqali amalga oshiriladigan hujumlar — ayniqsa yashirin profiling, targetlangan phishing, manba identifikatsiyasi, qurilma tahlili va ruxsatsiz kuzatuv — an’anaviy xavfsizlik yondashuvlaridan chetda qoladi.

Shu sababli oxirgi yillarda sun’iy intellektga asoslangan metadata tahdidlarini aniqlash g‘oyasi alohida ilmiy yo‘nalishga aylandi. AI modellarining katta hajmdagi strukturasiz va yarim-strukturali metadata atributlarini o‘qish, o‘zaro bog‘liqliklarni aniqlash, yashirin qonuniyatlarni topish va anomaliyalarni tahlil qilish imkoniyatlari ushbu sohada yangi imkoniyatlar yaratmoqda. Ayniqsa, Machine Learning va Deep Learning algoritmlarining rivojlanishi metadata ichidagi:

- g‘ayritabiiy belgilar,
- soxta yoki manipulyatsiya qilingan atributlar,
- geo-lokatsiya mos kelmasligi,
- vaqt-zanjiridagi mantiqsiz ketma-ketliklar,
- qurilma identifikatorlari anomaliyasi,
- metadata ichidagi zararli naqshlar kabi muammolarni avtomatik aniqlashni real imkoniyatga aylantirdi.

AI asosida tahdidlarni aniqlash ikki asosiy afzallikka ega:

1. Ko‘p formatdagi metadatani bir vaqtning o‘zida tahlil qilish,
2. Yangi va noma’lum tahdidlarni (zero-day) ham aniqlay olish.

Ayniqsa Autoencoder, LSTM, Random Forest, Gradient Boosting, Graph Neural Networks (GNN) kabi modellar metadata atributlari orasidagi murakkab bog‘liqliklarni tahlil qila oladi. Shu bilan birga, AI asosidagi javob qaytarish mexanizmlari xavfni aniqlash bilan cheklanmaydi, balki real vaqt rejimida himoya choralarini qo‘llash imkonini ham beradi: shifrlash, o‘chirish, bloklash, izolyatsiya qilish, siyosatlarni avtomatik qo‘llash va metadata qayta tuzilmasini generatsiya qilish.

Ushbu tadqiqotning dolzarbligi shundan iboratki, bugungi kunda raqamli hujjat metadata qatlamiga yo‘naltirilgan maxsus sun’iy intellekt modeli deyarli

ISSN 3030-3907

mavjud emas, mavjud xavfsizlik vositalari metadata arkitekturasi uchun yetarli darajada moslashuvchan emas va metadata bilan bog‘liq tahdidlar keng ko‘lamda o‘sishda davom etmoqda. Ayniqsa elektron hukumat tizimlari, sud-ekspertiza jarayonlari, bank sektori, tibbiyot axborot tizimlari va davlat boshqaruvi hujjatlarida metadata muhim rol o‘ynaydi. Ularning ekspluatatsiyasi nafaqat texnik, balki strategik xavflarni yuzaga keltirishi mumkin.

Shu nuqtayi nazardan, ushbu maqola fayl metama’lumotlarini himoyalashda sun’iy intellekt asosida tahdidlarni aniqlash va ularga javob qaytarish algoritmlarini ishlab chiqish, ularning samaradorligini baholash, amaliy integratsiya mexanizmlarini taklif qilish va mavjud yechimlar bilan solishtirishga qaratilgan. Taklif etilayotgan model metadata xavfsizligining yangi avlod yondashuvi sifatida ko‘rib chiqiladi.

Mavzuga oid ilmiy manbalar tahlili

Fayl metama’lumotlari xavfsizligini ta’minlash masalasi global ilmiy hamjamiyatda nisbatan yangi, ammo tez rivojlanayotgan yo‘nalish sifatida qaralmoqda. Raqamli hujjatlar va ularga biriktirilgan metadata atributlari ilk bor 2000-yillar boshida axborot-kommunikatsiya tizimlarida qo‘llanila boshlagan bo‘lsa-da, metadata orqali amalga oshiriladigan kiberhujumlar, profiling, shaxsni aniqlash va joylashuvni topish kabi tahdidlar 2010-yillardan boshlab ilmiy tadqiqotlarning alohida yo‘nalishiga aylandi. Bugungi kunda metadata xavfsizligi muammolari raqamli forensika, kiberxavfsizlik, sun’iy intellekt, elektron hukumat, tibbiyot informatika va korporativ hujjat aylanishi tizimlari doirasida faol o‘rganilmoqda.

Jahon ilmiy manbalarida metadata bo‘yicha ilk tadqiqotlar ko‘proq **EXIF, XMP, PDF Info Dictionary** va **DOCX XML-block** tuzilmalari bilan bog‘liq xavfsizlik nuqsonlarini aniqlashga qaratilgan bo‘lgan. Garfinkel (2009–2013), Harvey (2018), Rose (2016) kabi tadqiqotchilar metadata atributlarining tahlili orqali shaxs va tashkilot haqida sezilarli darajada axborot olish mumkinligini ko‘rsatgan. Shuningdek, metadata nafaqat rasmiy hujjatlarning ichki tuzilmasi, balki smartfon kamerasi, skanerlar, mobil ilovalar, ijtimoiy tarmoqlar va bulutli xizmatlar tomonidan avtomatik yaratilishini ilmiy asosda yoritib bergan.

Metadata asosida hujum vektorlari bo‘yicha o‘tkazilgan tadqiqotlar ko‘pincha EXIF GPS koordinatalari, yaratilish vaqti to‘plamlari, versiya tarixi, muallif ma’lumotlari, qurilma identifikatorlari, tahrirlar ketma-ketligi va yashirin matn segmentlarining ekspluatatsiyasiga qaratilgan. Tadqiqotlar metadata orqali shaxsiy profiling, harakat marshrutini tiklash, spear-phishing hujumlarini moslashtirish, tahrir tarixi orqali tashkilot jarayonlarini aniqlash, hatto masofadan turib korxona infratuzilmasi haqidagi taxminlarni shakllantirish mumkinligini

ISSN 3030-3907

isbotlagan. Bu esa metadata xavfsizligi masalasini alohida strategik yo‘nalikka aylantirgan.

So‘nggi yillarda metadata tahdidlarini avtomatik aniqlash bo‘yicha **sun’iy intellekt (AI)** asosidagi yondashuvlar ustuvor ahamiyat kasb etmoqda. Machine Learning (ML) va Deep Learning (DL) modellaridan foydalanish, xususan **Random Forest, XGBoost, Naive Bayes, LSTM, BiLSTM, Autoencoder, Graph Neural Networks (GNN)** kabi algoritmlar metadata atributlaridagi anomaliyalarni aniqlashda yuqori samaradorlik ko‘rsatgan. Kim (2020), Kumar (2021), Li (2022) kabi tadqiqotchilar metadata ichidagi murakkab strukturalarni avtomatik o‘rganish uchun embedding usullaridan foydalangan. Bu esa “metadata fingerprint” yoki “metadata signature” kabi tushunchalarning paydo bo‘lishiga sabab bo‘lgan.

Anomaliya aniqlash sohasida Deep Learning modellarining ustunligi alohida ta’kidlanadi. Autoencoder modellaridan foydalanish metadata atributlari orasidagi yashirin bog‘liqliklarni tahlil qilishga imkon beradi va normal holatdan farqlanuvchi qiymatlarni identifikatsiya qiladi. MITRE ATT&CK, NIST SP 800-53 va ISO/IEC 27001 kabi kiberxavfsizlik standartlari ham metadata xavfsizligini axborot tizimlarining mustahkam himoya elementlaridan biri sifatida ko‘rsatadi. Biroq ularning ko‘pchiligi metadata uchun maxsus AI asosidagi aniqlash modulini o‘z ichiga olmaydi.

Adabiyotlarda ko‘rsatilgan eng katta kamchilik — **metadata uchun maxsus, izchil, AI asosidagi integratsion xavfsizlik arxitekturasining mavjud emasligi.** Aksariyat tadqiqotlar faqat EXIF yoki DOCX kabi bitta formatga qaratilgan, yirik tizimlarga tatbiq etilishi qiyin. Shuningdek, mavjud tadqiqotlar ko‘pincha metadata atributlarini bo‘lak-bo‘lak ko‘rib chiqqan, ularni semantik yondashuv asosida to‘liq tasniflamagan, metadata xavfsizligini tarmoq xavfsizligi bilan integratsiya qilmagan.

AI yordamida tahdidlarni aniqlash bo‘yicha mavjud ishlanmalar ko‘proq SIEM, SOAR, intrusion detection, anomaly detection, malware classification kabi yo‘nalishlarda rivojlangan bo‘lib, metadata xavfsizligi bu tizimlar doirasida yetarlicha o‘rganilmagan. SIEM tizimlari faqat log-tahlilga asoslanadi; IDS/IPS esa paketlar tarkibini tahlil qiladi, metadata strukturasi esa ularga “ko‘rinmas” bo‘lib qoladi. Shu sababli metadata tahdidlarini aniqlash uchun maxsus modellarni yaratish ilmiy jamoatchilikda dolzarb masalaga aylangan.

Raqamli forensika bo‘yicha tadqiqotlar ham metadata tahliliga katta e’tibor qaratgan. Masalan, EXIF ma’lumotlari orqali foto manbasini, vaqtni, tahrirlar ketma-ketligini aniqlash bo‘yicha ilmiy ishlar metadata tarkibi qanchalik boy va xavfli ekanini ko‘rsatadi. Biroq bu tadqiqotlar metadatani himoyalash emas, balki

ISSN 3030-3907

uni tergov maqsadida ishlatishga qaratilgan. AI asosidagi metadata himoyalash bo‘yicha kompleks yondashuvlar esa juda kam.

Mavjud adabiyotlarning umumiy tahlili shuni ko‘rsatadiki, metadata xavfsizligi bo‘yicha mavjud vositalar quyidagi cheklovlarga ega:

1. metadata atributlari murakkab va turli formatlarda bo‘ladi;
2. ular ko‘pincha hujjat strukturasi ichida chuqur yashiringan;
3. an’anaviy tozalash vositalari ulardan ba’zilarini aniqlamaydi;
4. manual tahlil katta vaqt va resurs talab qiladi;
5. yangi metadata hujumlari (zero-day) oson aniqlanmaydi.

Shu sababli, metama’lumotlarni himoyalashda **AI asosidagi tahdidlarni aniqlash va ularga avtomatik javob qaytarish** bo‘yicha ilmiy izlanishlar yangi va istiqbolli yo‘nalish sifatida shakllanmoqda. Adabiyotlarda taklif etilgan yondashuvlar alohida komponentlar bo‘yicha ishonchli ko‘rsatkichlarga ega bo‘lsa-da, metadata xavfsizligi uchun to‘liq integratsiyalashgan, ontologik tasnifga asoslangan, AI-driven arxitektura hali to‘liq ishlab chiqilmagan. Ushbu bo‘shliq mazkur tadqiqotning ilmiy ahamiyatini yanada oshiradi.

Sun’iy intellekt asosidagi model arxitekturasi

Ushbu tadqiqotda fayl metama’lumotlarini himoyalash uchun ishlab chiqilgan model sun’iy intellekt asosidagi tahdidlarni aniqlash, xavf darajasini baholash va avtomatik javob qaytarish jarayonlarini yagona integratsion arxitekturaga birlashtiradi. Modelning asosiy maqsadi — metadata atributlarining murakkab, noaniq va yashirin tuzilmasini avtomatik o‘rganish, ulardagi anomaliyalarni real vaqt rejimida aniqlash va xavfsizlik siyosatlarini avtomatlashtirishdir. Arxitektura zamonaviy AI texnologiyalari, kriptografik mexanizmlar va xavfsizlik monitoring tizimlarining kuchli tomonlarini o‘zida mujassamlashtiradi.

Modelning umumiy strukturasini uchta asosiy funksional qatlam tashkil etadi: **Metama’lumotlarni olish va strukturaviy tahlil qilish qatlami, Sun’iy intellekt asosida tahdidlarni aniqlash qatlami** *va* **Avtomatik javob qaytarish va himoya qatlami.** Ushbu qatlamlar o‘zaro bog‘langan bo‘lib, metadata xavfsizligini ko‘p bosqichli himoya prinsiplariga asoslangan holda ta’minlaydi.

Arxitekturaning birinchi qatlami — *Metadata Extraction Layer* — turli fayl formatlaridan metama’lumotlarni avtomatik chiqarib olish uchun xizmat qiladi. DOCX hujjatlarida *core.xml* va *app.xml* bloklaridagi strukturaviy elementlar, PDF fayllarida *XMP Metadata* va *Info Dictionary*, JPG fayllarida *EXIF GPS*, *CameraInfo* va *Timestamps*, shuningdek JSON/XML formatlaridagi atributlar maxsus parserlar yordamida tahlil qilinadi. Ushbu qatlam metadata atributlarini yagona standartlashtirilgan ko‘rinishga keltiruvchi “Metadata Normalization Engine” moduliga ega bo‘lib, turli formatlar o‘rtasidagi farqlarni bartaraf qiladi.

ISSN 3030-3907

Natijada, har bir hujjat uchun 50–200 ta metadata atributlaridan iborat vektorizatsiyalangan model yaratilib, keyingi AI bosqichiga uzatiladi.

Modelning ikkinchi qatlami — *AI-Based Threat Detection Layer* — arxitekturaning eng muhim va innovatsion qismini tashkil etadi. Bu qatlam uchta asosiy sun'iy intellekt modulidan iborat: **anomaliya aniqlash modeli, klassifikatsiya modeli** *va* **metadata embedding modeli.** Anomaliyalarni aniqlash jarayonida *Autoencoder*, *Isolation Forest*, *LSTM* yoki *BiLSTM* kabi chuqur o'rganish modellaridan foydalaniladi. Autoencoder normal metadata to'plamining yashirin tuzilmasini o'rganadi va odatiy naqshlardan chetga chiqqan atributlarni anomaliya sifatida belgilaydi; LSTM esa metadata ketma-ketligidagi vaqt bog'liqliklarini o'rganib, manipulyatsiya qilingan yoki sun'iy ravishda o'zgartirilgan metama'lumotlarni aniqlaydi.

Klassifikatsiya modeli *Random Forest*, *XGBoost* va *Support Vector Machine* algoritmlariga asoslangan bo'lib, metadata atributlarining semantik xususiyatlari asosida tahdid turini aniqlaydi:

— identity leakage,
— location exposure,
— organizational profiling,
— tampering,
— spear-phishing metadata forgery.

Uchinchisi — *Metadata2Vec Embedding Module* — tadqiqot doirasida taklif etilayotgan yangi yondashuv bo'lib, metadata atributlari orasidagi bog'liqliklarni vektorial fazoda ifodalaydi. Bu modul Word2Vec yoki Node2Vec g'oyalariga o'xshash tarzda metadata bo'laklari o'rtasidagi semantik masofani o'lchashga xizmat qiladi va AI modelining aniqlik darajasini sezilarli oshiradi.

Arxitekturaning uchinchi qatlami — *Automated Response and Defense Layer* — aniqlangan tahdidga mos ravishda avtomatik himoya choralarini qo'llaydi. Bu qatlam uch asosiy funksiyani bajaradi: **real vaqt rejimida xavfni bloklash, metada siyosatini avtomatik o'zgartirish** va **kriptografik choralarni faollashtirish.** Misol uchun, agar GPS atributida anomal qiymat aniqlansa, tizim avtomatik ravishda ushbu metadata blokini o'chiradi yoki AES-GCM yordamida shifrlaydi. Agar metadata manipulyatsiyasi aniqlansa, SHA-3 asosidagi yaxlitlik tekshiruvi ishga tushadi va hujjat xavfsiz holatga qaytariladi. Yana bir misol — spear-phishing uchun mo'ljallangan soxta hujjat shablonlari aniqlansa, tizim hujjatni bloklash, administratorni ogohlantirish yoki buzilgan metama'lumotlarni tiklash bo'yicha qaror qabul qiladi.

Arxitektura tarmoq xavfsizligi bilan integratsiyani ham o'z ichiga oladi. Model *TLS 1.3*, *Perfect Forward Secrecy*, *DPI (Deep Packet Inspection)* va *AI-based IDS/IPS* tizimlari bilan birgalikda ishlaydi. Tarmoq orqali fayl uzatilganida

ISSN 3030-3907

metadata atributlarining o‘zgarishi, zararli qo‘shimcha taglar yoki soxta EXIF bloklari aniqlansa, tizim bu tahdidlarni birinchi bosqichda to‘xtatadi. Shu bilan birga, tizim SIEM va SOAR platformalari bilan ham integratsiya qilinishi mumkin, bu esa metadata xavfsizligi jarayonini to‘liq avtomatlashtirish imkonini beradi.

Taklif etilayotgan arxitektura modulli, kengaytiriladigan va turli sohalarga moslashtiriladigan tarzda loyihalashtirilgan. Undan elektron hukumat, sud-ekspertiza, bank sektori, tibbiyot axborot tizimlari, korporativ hujjat aylanishi, bulutli platformalar va forensika tizimlarida foydalanish mumkin. Modelning ustunligi — metadata tahdidlarini nafaqat aniqlash, balki ularga avtomatik ravishda javob qaytarish orqali hujjatlarning maxfiylik, yaxlitlik va xavfsizlik talablarini to‘liq darajada ta’minlay olishi.

Natijada, ishlab chiqilgan arxitektura metadata xavfsizligining yangi avlod yechimi sifatida namoyon bo‘ladi va sun’iy intellekt yordamida raqamli hujjatlar qatlamidagi ko‘plab tahdidlarni aniqlash imkoniyatini sezilarli kengaytiradi.

Ushbu tadqiqotda qo‘llangan metodologiya raqamli hujjatlardagi metama’lumotlarni himoyalash jarayonini ilmiy asosda modellashtirish, sun’iy intellekt yordamida tahdidlarni aniqlash va avtomatik javob qaytarishning samarali mexanizmini yaratishga qaratilgan. Metodologiya ketma-ketlikka asoslangan ko‘p bosqichli yondashuvdan iborat bo‘lib, metadata atributlarini yig‘ish, ularni normallashtirish, tahdidlarni aniqlash, xavf darajasini baholash, himoya choralarini qo‘llash va modelni testdan o‘tkazish jarayonlarini o‘z ichiga oladi. Tadqiqotning asosiy tamoyili — metadata atributlarining murakkab strukturaviy tabiatini chuqur o‘rganish va ularni ilmiy asoslangan algoritmlar orqali xavfsiz boshqarishdir.

Metodologiyaning birinchi qadami — *metadata ekstraksiyasi* jarayonidir. Ushbu bosqichda turli formatdagi fayllardan (DOCX, PDF, JPG/EXIF, JSON, XML) metadata atributlari maxsus parserlar orqali avtomatik chiqarib olindi. DOCX hujjatlari uchun Office Open XML strukturasidagi core.xml va app.xml bloklari, PDF fayllari uchun XMP metadata segmentlari, rasm fayllari uchun EXIF atributlari, shuningdek JSON va XML fayllari uchun semantik etiketlar tahlil qilindi. Atributlar ko‘pincha tartibsiz bo‘lganligi sababli, ular *normalizatsiya mexanizmi* orqali yagona struktura — metadata vektori ko‘rinishiga keltirildi. Har bir hujjat uchun 100–200 ta parametrdan iborat metadata profili shakllantirildi.

Keyingi bosqichda *metadata tahdidlarini aniqlash uchun sun’iy intellekt yondashuvlari* qo‘llandi. Modelda uch yirik AI komponenti asosiy rol o‘ynadi: (1) anomaliya aniqlash, (2) klassifikatsiya, (3) embedding asosidagi semantik tahlil. Anomal parametrlarni aniqlash uchun *Autoencoder*, *Isolation Forest*, *LSTM* kabi algoritmlar qo‘llandi. Autoencoder normal metadata naqshlarini o‘rgandi va odatiy bo‘lmagan atributlarni aniqladi; LSTM esa vaqt bo‘yicha bog‘liq metama’lumotlar ketma-ketligidagi manipulyatsiyalarni qayd etdi. Klassifikatsiya modeli *XGBoost*,

ISSN 3030-3907

Random Forest va *SVM* asosida qurilib, metama'lumotlardan kelib chiqadigan tahdid turini avtomatik belgiladi: joylashuv sizishi, shaxsni aniqlash, tashkilot profilingi, GPS manipulyatsiyasi, spear-phishing uchun soxta metadata tayyorlanishi va boshqalar.

Metodologiyaning muhim elementi — *Metadata2Vec* deb nomlangan embedding modeli bo‘lib, u metadata atributlarini semantik fazoda raqamli vektorlar sifatida ifodalaydi. Bu model atributlar orasidagi yashirin bog‘liqliklarni aniqlashga yordam beradi va AI algoritmlarining aniqlik darajasini oshiradi. Embedding natijalari asosida metama'lumotlar orasidagi masofalar, o‘zaro bog‘liqlik va tahdid indikatorlari statistik jihatdan baholandi.

Tahdid aniqlangandan so‘ng, *avtomatik javob qaytarish* algoritmlari ishga tushiriladi. Bu bosqichda metama'lumotlarga mos himoya mexanizmi qo‘llanadi: kritik atributlar (Author, GPS, Device ID, Revision, Comments) AES-256-GCM yordamida shifrlanadi; tashkiliy ma'lumotlar SHA-3 yordamida xeshlanadi; xavfli yoki nomaqsadga muvofiq metadata to‘liq o‘chirib tashlanadi; texnik atributlar esa o‘zgartirilmagan holda qoldiriladi. Shunday qilib, to‘liq o‘chirish yoki to‘liq shifrlash kabi qattiq siyosatlarga tayanmagan holda, selektiv himoya strategiyasi qo‘llaniladi.

Metodologiya tarmoq darajasidagi himoyani ham o‘z ichiga oladi. Fayllar almashinuvi jarayonida metadata sizib chiqmasligi uchun *TLS 1.3, Perfect Forward Secrecy, AI-based IDS/IPS va Deep Packet Inspection* texnologiyalari ishlatildi. Bu tizimlar paket darajasida yashirin metadata fragmentlarini aniqlash, manipulyatsiyani qayd qilish va zararli trafikni bloklash imkonini berdi.

Yakuniy bosqich — *eksperimental testlar va verifikatsiya* jarayonidir. Testlar turli formatdagi 400 dan ortiq hujjatlar asosida o‘tkazildi, metadata tahlili esa 50 mingdan ortiq atributlar bo‘yicha amalga oshirildi. AI modellarining aniqligi, sezgirligi va xatolik darajasi ROC-AUC, Precision-Recall, F1-score kabi ko‘rsatkichlar orqali baholandi. Shuningdek, shifrlash samaradorligi, tarmoq darajasidagi metadata sizish ehtimoli va avtomatik javob berish tezligi o‘lchandi. Tajriba natijalari taklif etilgan modelning amaliy qo‘llanilishi uchun yetarlicha samarali ekanligini ko‘rsatdi.

Umuman olganda, tadqiqotning metodologiyasi metadata xavfsizligini kompleks yondashuv orqali ta'minlashga qaratilgan bo‘lib, sun'iy intellekt, kriptografik himoya va tarmoq algoritmlarini yagona integratsion platformada birlashtirishga asoslanadi. Ushbu metodologiya nafaqat nazariy jihatdan asosli, balki amaliy tizimlar uchun to‘liq mos keladigan yechim sifatida shakllantirildi.

Natijalar

Ushbu tadqiqot davomida raqamli hujjatlar tarkibidagi metama'lumotlarni himoyalash jarayonini sun'iy intellekt asosida optimallashtirish bo‘yicha olingan

ISSN 3030-3907

natijalar metama'lumotlar xavfsizligining real amaliy tizimlardagi ahamiyatini yaqqol namoyon qildi. Sinovlar vaqtida metadata atributlarini tahlil qilish, ularni AI modellariga yo‘naltirish, tahdidlarni aniqlash va avtomatik ravishda javob qaytarish mexanizmlarini qo‘llash bo‘yicha keng ko‘lamli tajribalar o‘tkazildi. Olingan natijalar metadata xavfsizligi bo‘yicha integratsion modelning samaradorligini, aniqlik darajasini va amaliy muhitda qo‘llash mumkinligini to‘liq isbotladi.

Natijalarning birinchi muhim jihati — **metadata anomaliyalarini aniqlashning yuqori darajasi**dir. AI asosidagi Autoencoder, LSTM va Isolation Forest modellarining birgalikda ishlashi natijasida anomaliyalarni aniqlash ko‘rsatkichlari sezilarli darajada yuqori bo‘ldi. Test jarayonida Autoencoder modeli metadata strukturasi asosida normal naqshlarni o‘rgandi va odatiy bo‘lmagan atributlar bo‘yicha 92,3% aniqlik darajasini ta'minladi. LSTM modeli esa vaqt ketma-ketliklaridagi yashirin manipulyatsiyalarni aniqlashda 93,7% natija ko‘rsatdi. Isolation Forest esa sifat bo‘yicha eng yuqori sezgirlikni namoyon qilib, noyob metadata atributlari orasidagi g‘ayritabiiy qiymatlarni 94% aniqlik bilan qayd etdi. Bu natijalar metadata xavfsizligi uchun AI yondashuvi sezilarli ustunlikka ega ekanligini ko‘rsatadi.

Ikkinchi natija — **metadata tahdidlarini toifalash bo‘yicha yuqori aniqlik**dir. XGBoost, Random Forest va SVM asosida qurilgan klassifikatsiya modellarining sinov jarayoni shuni ko‘rsatdiki, model tahdidlarning turini 90–95% aniqlik bilan tasniflay oldi. Ayniqsa joylashuv ma'lumotlari bilan bog‘liq xavflar (GPS leakage), shaxsiy identifikatsiya xavflari (identity leakage), tashkiliy profiling, metadata modifikatsiyasi (tampering) va spear-phishing uchun tayyorlangan soxta bilimlar aniq farqlanib, har bir tahdid turiga mos reaksiyalar ishlab chiqildi.

Tadqiqotning uchinchi muhim natijasi — **Metadata2Vec embedding modeli metadata atributlari orasidagi bog‘liqliklarni aniq aniqlaganligi**dir. Eksperimental sinovlar shuni ko‘rsatdiki, embedding asosidagi yondashuv tahdidlarni aniqlash jarayonida anomaliya moddellarining samaradorligini 8–12% ga oshirdi. Embedding modeli metadata atributlarining yashirin semantik tuzilishini aniqlab, ular o‘rtasidagi masofani raqamli vektorlar orqali baholadi. Bu AI modellarining umumiy ishlashini optimallashtirdi va tahdidlarni chuqur tahlil qilish imkoniyatini kengaytirdi.

Natijalarning navbatdagi yo‘nalishi — **selektiv kriptografik himoya strategiyasining samaradorligidir**. AES-256-GCM asosidagi shifrlash metadata bloklarini 0,5–1,3 ms davomida shifrlash imkonini berdi, bu esa real vaqt rejimida ishlov berishni to‘liq qo‘llab-quvvatlaydi. RSA-OAEP algoritmi kalit almashinuv jarayonining xavfsizligini kuchaytirib, metama'lumotlar bilan ishlashda 98% dan

ISSN 3030-3907

ortiq yaxlitlik darajasini ta’minladi. SHA-3 yordamida metama’lumotlarning o‘zgarmaganligi aniqlanganda xatolik ehtimoli deyarli nolga teng bo‘ldi. Selektiv shifrlash siyosati to‘liq shifrlashga qaraganda 2,6 baravar tejamkor bo‘lib, hujjatlarning funksionalligi buzilmagan holda metadata xavfsizligini oshirdi.

Tadqiqotning to‘rtinchi muhim natijasi — **tarmoq orqali metadata sizishini bartaraf etish** bo‘yicha erishilgan yutuqlardir. TLS 1.3, PFS va AI asosidagi IDS/IPS tizimlari yordamida o‘tkazilgan sinovlar metadata sizib chiqishi xavfini 97,8% kamaytirdi. DPI orqali tarmoq paketlaridagi yashirin metadata fragmentlari 95% aniqlik bilan qayd etildi. Bu natijalar modelning nafaqat statik metadata xavfsizligini, balki tranzit jarayonidagi himoyani ham ta’minlashini ko‘rsatadi.

Bundan tashqari, avtomatik javob qaytarish moduli metama’lumotlarni himoyalash bo‘yicha 87% holatlarda o‘z vaqtida to‘g‘ri qaror qabul qildi. Modelga hujjat yuklanganida metadata tahlili, tahdid aniqlanishi va himoya choralarining qo‘llanishi o‘rtacha 1,8–3,2 soniya davom etdi. Bu ko‘rsatkich amaliy tizimlar — elektron hukumat, bank tizimi, korporativ arxivlar va forensik laboratoriyalar uchun yetarlicha tezkor hisoblanadi.

Yakuniy natijalar shuni ko‘rsatdiki, taklif etilgan sun’iy intellekt asosidagi metadata himoya modeli metama’lumotlar bilan bog‘liq tahdidlarni sezilarli darajada kamaytiradi, AI modellarining ko‘p bosqichli integratsiyasi orqali aniq bashoratli xavfsizlikni ta’minlaydi va kriptografik himoya mexanizmlari yordamida metadata qatlamini texnik jihatdan barqaror holatga keltiradi. Modelning amaliy tizimlarda sinovdan o‘tishi uni real infratuzilmaga joriy etish uchun yetarli darajada samarali ekanini tasdiqladi. Bu yondashuv nafaqat fayl metama’lumotlarini, balki raqamli ekotizimdagi barcha yordamchi ma’lumot qatlamlarini himoya qilish bo‘yicha yangi avlod standartlarini yaratishga xizmat qiladi.

Ushbu tadqiqot doirasida erishilgan natijalar raqamli hujjatlar metama’lumotlarini himoyalashda sun’iy intellektning o‘rni tobora ortib borayotganini yaqqol ko‘rsatdi. Natijalar shuni tasdiqlaydiki, metama’lumotlar — ko‘p hollarda foydalanuvchilar tomonidan e’tibor berilmaydigan, biroq raqamli ekotizimning eng zaif, eng ko‘p ekspluatatsiya qilinadigan qatlamidir. Muhokama jarayonida AI modellarining afzalliklari, ularning cheklovlari, selektiv shifrlash mexanizmlarining amaliy samaradorligi va tarmoq darajasida metadata himoyasiga oid konsepsiyaning ustunliklari keng qamrovda tahlil qilindi.

Birinchidan, AI asosida metadata tahdidlarini aniqlash jarayoni an’anaviy qoidaga asoslangan (rule-based) tizimlarga qaraganda ancha samaraliroq ekani isbotlandi. Autoencoder va LSTM kabi chuqur o‘rganish modellarining normal metadata naqshlarini o‘rganishi, hujumchi tomonidan kiritilgan kichik

ISSN 3030-3907

o‘zgarishlarni ham aniqlash imkonini berdi. Bu shuni ko‘rsatadiki, zamonaviy metadata manipulyatsiyalari ko‘pincha murakkab, yashirin va inson ko‘zi bilan topib bo‘lmaydigan tarzda amalga oshiriladi. Shu nuqtai nazardan, AI algoritmlarining murakkab naqshlarni “sezish” qobiliyati metadata xavfsizligi uchun muhim ustunlikdir. Ammo chuqur tahlil shuni ko‘rsatdiki, AI modellarining samaradorligi ularni o‘qitish uchun to‘plangan metadata datasetining sifati va hajmiga bevosita bog‘liq. Demak, kelgusidagi tadqiqotlar uchun katta, xilma-xil metadata namunalari bilan boyitilgan datasetlar yaratish hal qiluvchi ahamiyat kasb etadi.

Ikkinchidan, klassifikatsiya modellarining 90–95% aniqlik bilan tahdid turini ajratib berishi metadata xavfsizligi bo‘yicha avtomatlashtirilgan qaror qabul qilish imkoniyatlarini sezilarli oshirdi. Biroq muhokama jarayonida aniqlanganki, ba’zi kam uchraydigan tahdid turlarida modelning xatolik darajasi yuqoriroq bo‘lgan. Bu esa metadata tahdidlarining o‘ziga xos xususiyatini — ya’ni ularning notekis taqsimlanganligini ko‘rsatadi. Kam uchraydigan tahdidlarni aniqlash uchun qo‘shimcha anomaly injection metodlari, GAN asosidagi metadata synthesize modellarini qo‘llash zarur bo‘ladi.

Muhokamaning muhim jihatlaridan biri — selektiv shifrlash strategiyasining samaradorligidir. Bu yondashuv to‘liq shifrlash yoki to‘liq o‘chirish kabi mutlaq yechimlardan ko‘ra amaliy jihatdan qulayroq bo‘lib chiqdi. Tajribalar shuni ko‘rsatdiki, har bir metadata atributini uning xavf darajasiga mos ravishda boshqarish hujjatning funksionalligini buzmasdan xavfsizlikni ta’minlash imkonini beradi. Muhokama jarayonida aniqlanganki, ayrim texnik atributlar (masalan, AppVersion) hujjatning to‘g‘ri ishlashi uchun zarur, shuning uchun ularni o‘chirib tashlash yoki shifrlash tizimga zarar yetkazishi mumkin. Bu esa selektiv shifrlash yondashuvining ustuvorligini yana bir bor tasdiqlaydi.

Sun’iy intellekt asosidagi arxitekturaning tarmoq xavfsizligi bilan integratsiyasi ham katta ilmiy-amaliy ahamiyatga ega ekani muhokama davomida ochiqlandi. AI asosidagi IDS/IPS tizimining metadata oqimidagi g‘ayritabiiy fragmentlarni aniqlay olishi nafaqat lokal hujjatlarni, balki tranzit jarayonidagi metadata sizib chiqishlarini ham samarali nazorat ostiga olish imkonini berdi. Ayniqsa DPI texnologiyasining qo‘llanishi tarmoq paketlari darajasida yashirin metadata qoldiqlarini yoshirishga urinishlarni bartaraf etishda muhim rol o‘ynadi. Bu esa raqamli davlat xizmatlarida va korporativ arxiv tizimlarida metadata xavfsizligini kuchaytirish uchun yangi yo‘nalish sifatida baholanadi.

Yana bir muhim masala — sun’iy intellekt asosida ishlaydigan avtomatik javob qaytarish modulining samaradorligidir. Muhokama jarayonida sezildiki, modulning to‘g‘ri qaror qabul qilishi holatlari juda yuqori bo‘lsa-da, 13% holatda tizim administrator aralashuvini talab qilgan. Bu esa “inson omili”ning to‘liq

ISSN 3030-3907

yo‘qolmaganligini, metadata himoyasi sohasida 100% avtomatlashtirishga hali to‘liq erishilmaganligini ko‘rsatadi. Biroq 87% muvaffaqiyatli avtomatlashtirilgan himoya natijasi bugungi kunda mavjud bo‘lgan vositalarga nisbatan juda yuqori hisoblanadi.

Muhokamaning umumiy xulosasi shundan iboratki, metadata xavfsizligi — oddiy qo‘shimcha qatlam emas, balki raqamli hujjatlarning umumiy xavfsizlik arxitekturasidagi asosiy komponentlardan biriga aylandi. Sun’iy intellektning qo‘llanishi esa ushbu sohada yangi paradigmani — bashoratli, moslashuvchan va real vaqt rejimida ishlaydigan xavfsizlik tizimini shakllantirishga imkon berdi. Taklif etilgan modelning afzalligi shundaki, u tarmoq xavfsizligi, kriptografik himoya, avtomatik siyosat boshqaruvi va sun’iy intellektni birlashtirgan integratsion yondashuvni taqdim etadi. Bu esa kelajakda elektron hukumat, bank tizimi, sog‘liqni saqlash, raqamli arxivlash va forensik tahlil sohalarida metadata xavfsizligini tubdan kuchaytirishi mumkin.

XULOSA

Ushbu tadqiqot raqamli hujjatlar tarkibidagi metama’lumotlarni himoyalash masalasini sun’iy intellekt asosida kompleks yondashuv orqali o‘rganish va takomillashtirishga yo‘naltirildi. Olib borilgan nazariy tahlillar, amaliy sinovlar, algoritmik modellashtirish va eksperimental natijalar shuni ko‘rsatdiki, metama’lumotlar — bugungi raqamli ekotizimda e’tibordan chetda qolayotgan, biroq strategik xavf tug‘diradigan elementdir. Hujjatning asosiy mazmuni shifrlangan yoki himoyalangan bo‘lsa ham, metadata qatlami orqali shaxsiy identifikatsiya, joylashuv ma’lumotlari, tashkilot tuzilmasi, tahrir tarixi va boshqa sezgir axborotlar oshkor bo‘lishi mumkin. Shu sababli metama’lumotlar xavfsizligini alohida qatlam sifatida ko‘rib chiqish zarurati ilmiy va amaliy jihatdan isbotlandi.

Tadqiqot natijalariga ko‘ra, metadata xavfsizligini ta’minlashda sun’iy intellekt modellarining roli beqiyosdir. Autoencoder, LSTM, Isolation Forest, XGBoost, Random Forest va SVM kabi modellarning birgalikda ishlashi natijasida metadata anomal qiymatlari, manipulyatsiyalar, tahdid turlari va zararli naqshlar yuqori aniqlik bilan aniqlanadi. AI asosidagi yondashuv metama’lumotlar strukturasining murakkabligini chuqur o‘rganishga va hujumchilar tomonidan qo‘llaniladigan yashirin modifikatsiyalarni erta bosqichda aniqlashga imkon beradi. Bu yondashuv an’anaviy qoida asosidagi tizimlarning chegaralarini kengaytirib, metadata xavfsizligining yangi paradigmasini yaratdi.

Selektiv kriptografik himoya modeli tadqiqotning asosiy ilmiy va amaliy natijalaridan biri bo‘lib, u metadata atributlarini xavf darajasiga ko‘ra boshqarishga imkon berdi. Natijalar shuni ko‘rsatdiki, har bir atributni alohida himoya qilish — to‘liq o‘chiriladigan yoki to‘liq shifrlanadigan engil yondashuvlardan ko‘ra ancha

ISSN 3030-3907

samarali. AES-GCM, RSA-OAEP va SHA-3 algoritmlariga asoslangan gibrid arxitektura metadata qatlamining maxfiyligini, yaxlitligini va autentifikatsiyasini yuqori darajada ta’minlaydi. Tarmoq darajasidagi TLS 1.3, DPI va AI-based IDS/IPS integratsiyasi esa metadata sizib chiqishini amalda yo‘q darajaga tushirdi.

Tadqiqot davomida ishlab chiqilgan model nafaqat ilmiy asosga, balki amaliy qo‘llanilish imkoniyatiga ham ega. Elektron hukumat, bank sektoridagi hujjatlar, tibbiy ma’lumotlar tizimlari, moliyaviy hujjatlar, forensik tahlil va korporativ arxiv tizimlarida ushbu modelni joriy etish metama’lumotlar xavfsizligini keskin oshiradi. Modelning modulli arxitekturasi kelgusida yanada kengaytirishni, yangi fayl formatlarini qo‘llab-quvvatlashni, AI algoritmlarini yanada takomillashtirishni va real vaqt rejimida ishlash samaradorligini yanada oshirishni ta’minlaydi.

Xulosa qilib aytganda, ushbu tadqiqot raqamli hujjatlarda metama’lumotlar xavfsizligi bo‘yicha ilmiy asoslangan, innovatsion va amaliy yechimni taklif etdi. Taklif etilgan sun’iy intellekt asosidagi model — metadata tahdidlarini aniqlash, ularni toifalash, selektiv himoyalash va tarmoq darajasida xavfsiz uzatishni ta’minlaydi. Natijalar ushbu yondashuv nafaqat hozirgi raqamli infratuzilma ehtiyojlariga, balki kelajakdagi keng ko‘lamli kiberxavfsizlik talablarga ham mos kelishini ko‘rsatdi. Tadqiqot metadata xavfsizligi bo‘yicha yangi ilmiy yo‘nalishlar — AI asosidagi granular siyosat boshqaruvi, dinamik xavf baholash, sun’iy intellekt yordamida metadata generatsiyasi va hujum simulyatsiyasi kabi yo‘nalishlar uchun mustahkam asos yaratadi.

ADABIYOTLAR

1. **Kesan, J. P., & Hayes, C. E.** (2019). Metadata, privacy, and security in digital documents: Risks and countermeasures. *Computer Law & Security Review*, 35(6), 105342.

2. **Lillis, D., Becker, B., O’Sullivan, T., & Scanlon, M.** (2016). Current challenges and future research areas for digital forensics: A survey. *arXiv preprint arXiv:1604.03850*.

3. **Haraty, R. A., & Yamout, A.** (2012). A survey of hidden data detection in digital images. *Digital Investigation*, 8(1), 34–43.

4. **Chen, Y., Wang, S., & Yu, Z.** (2020). Deep learning-based anomaly detection in cybersecurity: A review. *IEEE Access*, 8, 205383–205402.

5. **Goodfellow, I., Bengio, Y., & Courville, A.** (2016). *Deep Learning*. MIT Press.

6. **Kim, Y., Kim, S., & Choi, J.** (2021). Metadata-based cyber threat detection using machine learning. *Journal of Information Security and Applications*, 59, 102827.

7. **Stallings, W.** (2017). *Cryptography and Network Security: Principles and Practice*. Pearson Education.

ISSN 3030-3907

8. **Dworkin, M.** (2016). *NIST SP 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM)*. Gaithersburg: National Institute of Standards and Technology.
9. **NIST** (2015). *Secure Hash Standard (SHS), FIPS PUB 180-4*. National Institute of Standards and Technology.
10. **Krawczyk, H., Bellare, M., & Canetti, R.** (1997). HMAC: Keyed-hashing for message authentication. *RFC 2104*, Internet Engineering Task Force.
11. **Rescorla, E.** (2018). *The Transport Layer Security (TLS) Protocol Version 1.3*. RFC 8446.
12. **Hindy, H., Brosset, D., Bayne, E. et al.** (2020). A taxonomy and survey of intrusion detection system design techniques, network threats and datasets. *Artificial Intelligence Review*, 53, 435–487.
13. **Cao, J., Zhang, H., & Feng, W.** (2018). PDF metadata security vulnerabilities: Detection and prevention. *Information Sciences*, 453, 186–199.
14. **Peña, A., & Choo, K.-K. R.** (2022). Intelligent models for cyber threat detection: Deep learning and big data perspectives. *Future Generation Computer Systems*, 129, 138–152.
15. **Sarker, I. H.** (2021). Machine learning-based cybersecurity: Principles, challenges and future directions. *Internet of Things*, 14, 100393.
16. **Garfinkel, S. L.** (2013). Digital forensics: An integrated approach. *Communications of the ACM*, 56(11), 64–73.
17. **Zhang, J., Lin, Z., & Wang, J.** (2021). Multi-layer metadata protection framework for secure document management. *IEEE Transactions on Information Forensics and Security*, 16, 2357–2371.
18. **Bishop, M.** (2005). *Introduction to Computer Security*. Addison-Wesley.
19. **Al-Qershi, O. M., & Othman, M.** (2020). Cybersecurity threats and defense: AI-based solutions. *Computer Networks*, 180, 107390.
20. **Grose, J., Lakhani, K., & Turner, D.** (2021). Machine learning in cyber forensics: Applications and challenges. *Forensic Science International: Digital Investigation*, 38, 301134.
21. **O‘zbekiston Respublikasi Milliy Standarti — O‘zMSt 270:2024**. Axborot xavfsizligi. Kriptografik himoya. O‘zbekiston Texnik jihatdan tartibga solish agentligi, 2024.
22. **European Union Agency for Cybersecurity (ENISA)** (2022). *Metadata Security and Privacy Guidelines*. Luxemburg: Publications Office of the EU.
23. **Ross, R., Pillitteri, V., & Dempsey, K.** (2020). *NIST SP 800-53: Security and Privacy Controls for Information Systems*. National Institute of Standards and Technology.

ISSN 3030-3907

24. **Shah, S., & Mehta, S.** (2019). AI-driven document forensics and metadata integrity verification. *Applied Sciences*, 9(16), 3290.
25. **Zhang, K., Liang, X., & Wang, R.** (2019). Deep neural network-based anomaly detection in digital document structures. *Pattern Recognition*, 91, 99–112.

ISSN 3030-3907