“RAQAMLI HUJJATLARDA METAMA’LUMOTLARNI HIMOYALASH UCHUN KRIPTOGRAFIK MODELLAR VA TARMOQ XAVFSIZLIGI ALGORITMLARINING INTEGRATSIYASI”

Sodiqova Dilnoza Jumanazarovna

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

Email: sodiqovadilnoza655@gmail.com

Annotatsiya. Mazkur ilmiy ishda raqamli hujjatlar tarkibidagi metama’lumotlarni himoyalashga qaratilgan integratsiyalashgan kriptografik va tarmoq xavfsizligi modeli ishlab chiqilgan. Metama’lumotlar — muallif, yaratilgan vaqt, GPS koordinatalar, qurilma identifikatori, versiya tarixi va boshqa texnik atributlar — ko‘pincha asosiy mazmunda bo‘lmagan holda sezgir ma’lumotlarni oshkor qiladi. Shuning uchun metama’lumotlar qatlamini alohida himoyalash bugungi axborot-kommunikatsiya tizimlarida muhim talab hisoblanadi. Taklif etilgan model AES-GCM algoritmi asosida simmetrik shifrlash, RSA-OAEP orqali kalitlar almashinuvi, SHA-3 yordamida yaxlitlikni tekshirish, TLS 1.3 asosidagi tranzit xavfsizligi, IDS/IPS tizimlari orqali tarmoqdagi anomaliyalarni aniqlash hamda ontologik metama’lumotlar tasnifi orqali selektiv shifrlash mexanizmlarini o‘z ichiga oladi. Eksperimental natijalar metadata shifrlash samaradorligini, tarmoq orqali uzatishda xavfsizlikning oshishini va metama’lumotlar bilan bog‘liq tahdidlarning keskin kamayishini ko‘rsatdi. Model O‘zbekistonda qabul qilingan O‘zMSt 270:2024 kriptografik standartlari bilan mos keladi hamda elektron hukumat, sog‘liqni saqlash, moliyaviy texnologiyalar va raqamli arxivlash bo‘yicha amaliy joriy etish imkoniyatiga ega.

Kalit so‘zlar: metama’lumotlar, kriptografiya, AES-GCM, RSA-OAEP, SHA-3, selektiv shifrlash, ontologik tasnif, tarmoq xavfsizligi, TLS 1.3, IDS/IPS, raqamli hujjatlar, metadata himoyasi,

Аннотация. В данной научной работе разработана интегрированная модель криптографической и сетевой безопасности, направленная на защиту метаданных, содержащихся в цифровых документах. Метаданные — такие как сведения об авторе, время создания, GPS-координаты, идентификатор устройства, история версий и другие технические атрибуты — нередко раскрывают конфиденциальную информацию, несмотря на то что они не относятся к основному содержанию файла. Поэтому защита слоя метаданных является важным требованием современных информационно-коммуникационных систем. Предложенная модель включает симметричное шифрование на основе AES-GCM, безопасный обмен ключами через RSA-OAEP, проверку целостности с использованием SHA-3, защиту передачи данных на основе протокола TLS 1.3, обнаружение сетевых аномалий с

ISSN 3030-3907

помощью систем IDS/IPS, а также селективное шифрование метаданных, реализованное через онтологическую классификацию. Экспериментальные результаты продемонстрировали эффективность шифрования метаданных, повышение защищённости при передаче данных по сети и существенное снижение связанных с метаданными угроз. Модель соответствует национальному криптографическому стандарту O‘zMSt 270:2024 и может быть практически применена в электронном правительстве, здравоохранении, финансовых технологиях и цифровом архивировании.

Ключевые слова : метаданные, криптография, AES-GCM, RSA-OAEP, SHA-3, селективное шифрование, онтологическая классификация, сетевая безопасность, TLS 1.3, IDS/IPS, цифровые документы, защита метаданных

Abstract. This research develops an integrated cryptographic and network security model aimed at protecting metadata embedded within digital documents. Metadata — such as author information, creation time, GPS coordinates, device identifiers, version history, and other technical attributes — often reveal sensitive information despite not being part of the document’s main content. Therefore, protecting the metadata layer has become a critical requirement in modern information and communication systems. The proposed model incorporates symmetric encryption using AES-GCM, secure key exchange through RSA-OAEP, integrity verification based on SHA-3, transit protection supported by TLS 1.3, network anomaly detection via IDS/IPS systems, and selective metadata encryption enabled by ontology-based classification. Experimental results demonstrate the effectiveness of metadata encryption, improved security during network transmission, and a significant reduction of metadata-related risks. The model complies with the national cryptographic standard O‘zMSt 270:2024 and can be practically implemented in e-government services, healthcare information systems, financial technologies, and digital archiving infrastructures.

Keywords: metadata, cryptography, AES-GCM, RSA-OAEP, SHA-3, selective encryption, ontological classification, network security, TLS 1.3, IDS/IPS, digital documents, metadata protection

Kirish.

Axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi global miqyosda raqamli hujjatlardan foydalanish hajmini keskin oshirdi. Bugungi kunda davlat boshqaruvi, bank tizimlari, sog‘liqni saqlash, ta’lim sektori, sanoat, korporativ boshqaruv va hatto kundalik aloqalar ham elektron shakldagi hujjatlarga asoslanadi. Raqamli hujjatlarning qulayligi va tezkorligi ularni hayotning barcha jabhalarida ajralmas vositaga aylantirdi. Shu bilan birga, hujjatlarning ko‘zga ko‘rinmas, ammo juda muhim qatlami — metama’lumotlar (metadata) — ko‘plab

ISSN 3030-3907

foydalanuvchilar, hattoki mutaxassislar tomonidan yetarlicha baholanmayotgan xavf omiliga aylangan.

Metama'lumotlar hujjatning o'zi emas, balki hujjat haqida ma'lumot beruvchi qo'shimcha texnik va kontekstual atributlardir. PDF, DOCX, JPG yoki boshqa formatlar tarkibida muallif nomi, tashkilot, qurilma identifikatori, GPS koordinatalari, yaratilish va tahrir sanasi, versiya tarixi, dastur versiyasi, foydalanuvchi akkaunti, yashirin struktura elementlari va boshqa ko'plab ma'lumotlar avtomatik tarzda saqlanadi. Mazkur metadata komponentlari dastlab hujjatni boshqarish, versiyalarni kuzatish, mualliflikni aniqlash yoki texnik protseduralarni yengillashtirish uchun yaratilgan bo'lsa-da, bugungi kunda ular kiberjinoyatchilar va razvedka tizimlari uchun juda qulay hujum manbalaridan biriga aylangan.

Metama'lumotlar ekspluatatsiya qilinganda shaxsni identifikatsiya qilish, tashkilot ichki tuzilmasini aniqlash, xodimlar faoliyatini vaqt bo'yicha tiklash, geolokatsiyani aniqlash, ijtimoiy muhandislik hujumlarini tayyorlash, spear-phishing hujumlarini aniq yo'naltirish, shantaj va doxxing kabi xatarlar yuzaga keladi. Shuning uchun global axborot xavfsizligi ekotizimida metadata allaqachon "yashirin hujum vektori" sifatida tan olingan.

Hujjat mazmuni shifrlangan yoki parol bilan himoyalangan bo'lsa ham, metama'lumotlar ko'pincha ochiq va o'qilishi mumkin bo'lgan holda qoladi. Ya'ni kontentni yashirish foyda bermaydi — ko'pincha metadata orqali sezilarli darajada maxfiy ma'lumotlar sizib chiqadi. Bu esa raqamli hujjatlar xavfsizligiga oid yondashuvlarni tubdan qayta ko'rib chiqishni talab qiladi.

O'zbekiston Respublikasida ushbu mavzuning ahamiyati yanada kattaroq. Raqamli transformatsiya siyosati — "Raqamli O'zbekiston – 2030" strategiyasi asosida — davlat xizmatlari, bank tizimi, sog'liqni saqlash, ta'lim va biznes jarayonlarda elektron hujjat aylanishini joriy qilishni jadallashtirdi. My.gov.uz, id.egov.uz, epay.gov.uz, EMR, LMS, elektron shartnomalar va raqamli arxiv tizimlari kabi platformalar millionlab raqamli hujjatlarni qayta ishlamoqda. Demak, ularga biriktirilgan metama'lumotlar ham millionlab birlikdan iborat bo'lib, ulardagi har qanday sizish davlat xavfsizligi, moliyaviy barqarorlik va fuqarolarning shaxsiy hayotiga bevosita tahdid tug'diradi.

Amaldagi metama'lumotlarni tozalash vositalari ko'plab cheklovlarga ega: ular hujjat funksionalligini buzadi, barcha turdagi metadata atributlarini bir xil usulda o'chiradi, hujjat strukturasi izdan chiqishi mumkin, hamma formatlarni to'liq qo'llab-quvvatlamaydi, korporativ tizimlarda esa qo'lda boshqarish imkonsizdir. Eng muhim muammo — metadata tranzit jarayonida (hujjat tarmoqdan o'tganda) baribir himoyalanmay qolishi.

ISSN 3030-3907

Shu sababli yangi avlod yondashuvi zarur: metama'lumotlarni selektiv boshqarish, xavf darajasiga qarab turli kriptografik mexanizmlarni qo'llash, hujjat mazmunini buzmasdan himoya darajasini oshirish, tarmoq xavfsizligini ham integratsiya qilish hamda barcha jarayonlarni ontologik siyosat orqali avtomatlashtirish.

Taklif etilayotgan selektiv kriptografik himoya modeli aynan mana shu ehtiyojdan kelib chiqqan. Model's asosiy g'oyasi shundan iboratki: barcha metadata teng emas; demak, ular uchun turli darajadagi himoya mexanizmlari qo'llanishi lozim. Shaxsiy identifikatsiya atributlari to'liq shifrlanadi, joylashuv ma'lumotlari yaxlitlik nazorati bilan tekshiriladi, organisatorik metadata xeshlanadi, texnik atributlar o'z holida qoldiriladi. AES-GCM, RSA-OAEP, SHA-3, TLS 1.3 va IDS/IPS kabi texnologiyalarning birgalikda qo'llanishi esa metadata xavfsizligini nafaqat saqlash, balki uzatish jarayonida ham ta'minlaydi.

Tadqiqotning ilmiy yangiligi — metadata xavfsizligi bo'yicha mavjud yondashuvlar orasida eng mukammal hisoblangan selektiv shifrlashning ontologik boshqaruv bilan integratsiya qilinishi, milliy kriptografik standartlar bilan mosligi, real tizimlarga qo'llash imkoniyatining kengligi va metadata ekspluatatsiyasiga qarshi kompleks himoya mexanizmlarini shakllantirishdadir.

Kirish bo'limidan xulosa sifatida aytish mumkinki, raqamli hujjatlarning metama'lumotlari bugungi kunda axborot xavfsizligining eng nozik va strategik jihatlaridan biri bo'lib, ularni himoyalash O'zbekistonning raqamli iqtisodiyoti barqarorligi, davlat boshqaruvi xavfsizligi va fuqarolar shaxsiy hayotining daxlsizligini ta'minlash uchun muhim ahamiyatga ega. Shu asosda, keyingi bo'limlarda metama'lumotlarning himoyasi bo'yicha amaldagi yondashuvlar, texnologiyalar, tahdidlar va taklif qilinayotgan integratsion kriptografik modelning metodologiyasi chuqur tahlil qilinadi.

Metama'lumotlar xavfsizligi bo'yicha ilmiy manbalar tahlili

Raqamli hujjatlar va ularning tarkibida saqlanadigan metama'lumotlarni himoyalash masalasi xalqaro ilmiy adabiyotlarda so'nggi yillarda tez sur'atlarda rivojlanayotgan, ko'p qirrali tadqiqot yo'nalishlaridan biri sifatida e'tirof etilgan. Umuman olganda, metadata tushunchasi dastlab kutubxonashunoslik va ma'lumotlar kataloglash tizimlaridan kelib chiqqan bo'lsa-da, bugungi raqamli transformatsiya jarayonlari uning xavfsizlikdagi o'rni va rolini tubdan o'zgartirdi. Raqamli hujjatlarning o'zida ko'zga tashlanmaydigan ko'plab texnik atributlar mavjud bo'lib, ular dasturiy, kontekstual yoki identifikatsion ma'lumotlarni o'z ichiga oladi. Xalqaro ilmiy tadqiqotlarda ushbu atributlar yomon niyatli shaxslar tomonidan ekspluatatsiya qilinganda identifikatsiya qilish, ijtimoiy muhandislikni kuchaytirish, xodimlar faoliyatini kuzatish, joylashuvni aniqlash, tashkilot ichki

ISSN 3030-3907

tizimlarini xaritalash yoki maxfiy obyektlar haqida bilvosita ma’lumot to‘plash kabi xavfli jarayonlar yuzaga kelishi isbotlangan.

Ko‘plab ilmiy manbalarda Microsoft Office, PDF, va EXIF formatlaridagi metama’lumotlarning xavf darajasi alohida ta’kidlanadi. DOCX hujjatlaridagi core.xml va docProps fayllarida saqlanadigan “Author”, “Company”, “Manager”, “LastModifiedBy”, “RevisionTime” kabi atributlar profiling hujumlarida asosiy manba bo‘lishi mumkin. PDF hujjatlarida esa XMP metadata bloklari kontentdan mustaqil tarzda saqlanishi bois, hatto fayl tozalansa ham, texnik atributlarning bir qismi hujjat ichida yashirin ko‘rinishda qolishi mumkin. EXIF rasm metama’lumotlari esa dunyo ilmiy doirasida eng xavfli metadata turlaridan biri sifatida e’tirof etiladi, chunki GPS koordinatalari yordamida shaxsning harakat marshruti, manzili, hatto maxfiy obyektlar joylashuvi aniqlanishi mumkin.

Adabiyotlar shuni ko‘rsatadiki, mavjud amaliy vositalar — MAT2, ExifTool, MetadataCleaner kabi dasturlar metadata xavfsizligini ta’minlashda muhim rol o‘ynasa-da, ular asosan *tozalash* (ya’ni metama’lumotlarni butunlay o‘chirib tashlash) tamoyiliga asoslanadi. Biroq, ko‘plab hujjat turlari to‘liq metadata o‘chirib tashlashga mos emas, chunki ayrim texnik atributlar tizimning ishlashi uchun zarur bo‘ladi. Bundan tashqari, mavjud vositalarning aksariyati korporativ siyosatlarni qo‘llamaydi, selektiv boshqaruv mexanizmiga ega emas, tarmoq xavfsizlik algoritmlari bilan integratsiyalashmagan hamda kriptografik modul bilan birgalikda ishlash imkoniyatidan yiroqdir. Shu sababli, ilmiy manbalarda metadata himoyasini to‘liq ta’minlash uchun ko‘proq kriptografik yondashuvlarga e’tibor qaratish zarurligi qayd etilgan.

Kriptografiya bo‘yicha eng nufuzli manbalarda AES-GCM, RSA-OAEP, ECC kabi algoritmlarning integratsiyasi metama’lumotlarni himoyalashda samarali hisoblanadi. AES-GCM o‘zining muhim xususiyatlari — shifrlash va autentifikatsiya bir vaqtning o‘zida amalga oshirilishi — tufayli metadata bloklarini selektiv shifrlashda eng maqbul variant sifatida ko‘rsatilgan. RSA-OAEP esa sessiya kalitini xavfsiz uzatish uchun eng ishonchli usullardan biri sifatida keng tavsiya etiladi. SHuningdek, NIST tomonidan tavsiya etilgan SHA-3 xesh algoritmi sifat jihatidan yuqori bo‘lib, metadata yaxlitligini tekshirish uchun samarali hisoblanadi. Xalqaro adabiyotlarda metadata xavfsizligini ta’minlashda aynan shu gibrid kriptografik sxemalardan foydalanish tavsiya etiladi.

Tarmoq xavfsizligi bo‘yicha manbalarda TLS 1.3 protokoli metadata tranzitda shifrlangan holda uzatilishining eng yaxshi yo‘li sifatida ko‘rsatiladi. Zero, TLS 1.3 avvalgi protokollardagi barcha zaif modul va mexanizmlarni bartaraf etgan, Perfect Forward Secrecy xususiyati esa kalitlar o‘g‘irlanganda ham avvalgi sessiyalarni ochishga imkon bermaydi. IDS/IPS tizimlari bo‘yicha ilmiy adabiyotlarda esa metadata oqimlarida g‘ayritabiiy signallarni aniqlash — ayniqsa

ISSN 3030-3907

hujjatlar ketma-ketligi yoki rasm metama'lumotlari orqali tarqalish ketma-ketligi — kiberhujumlarni erta aniqlashga yordam berishi ta'kidlangan.

Metama'lumotlarni semantik boshqarish bo'yicha eng yangi ilmiy tadqiqotlar ontologik modellarga e'tibor qaratadi. Ontologiyalar RDF, OWL kabi formatlarda metadata atributlarini tarkibiy-guruhli tasniflash, ularning xavf darajasini belgilash, selektiv shifrlash siyosatini avtomatlashtirish va domenlarga xos (bank, tibbiyot, davlat xizmatlari) xavfsizlik qoidalarini yaratishga imkon beradi. Ontologik yondashuv ilmiy adabiyotlarda metama'lumotlarni to'liq o'chirishga emas, balki ularni *semantik boshqaruv asosida himoyalashga* qaratilgan eng zamonaviy metod sifatida ko'rsatiladi.

O'zbekistonda metadata xavfsizligi bo'yicha ilmiy adabiyotlar hali ko'p emas, ammo "Raqamli O'zbekiston – 2030" strategiyasi, O'zMSt 270:2024 kriptografik standarti, UZCERT hisobotlari, TATU va boshqa ilmiy muassasalarda olib borilayotgan tadqiqotlar bu yo'nalishda izchil rivojlanish borligini ko'rsatadi. Ammo adabiyotlarda metama'lumotlarni to'liq kriptografik tarzda shifrlash, tarmoq xavfsizligi algoritmlari bilan integratsiyalashgan yondashuvning yetishmasligi, selektiv shifrlash mexanizmlarining kam tadqiq etilgani, kalit boshqaruvi bo'yicha amaliy tavsiyalarning yetarli emasligi ilmiy bo'shliq sifatida qayd etiladi.

Umuman olganda, mavjud ilmiy manbalar metadata xavfsizligini bir necha yo'nalishda o'rgangan bo'lsa-da, integratsiyalashgan — ya'ni kriptografiya, ontologik siyosat, tarmoq xavfsizligi, yaxlitlikni tekshirish hamda amaliy joriy etish mexanizmlarini o'z ichiga olgan kompleks yondashuv — hozircha yetarli darajada ishlab chiqilmagan. Shuning uchun ushbu tadqiqot aynan mana shu bo'shliqni to'ldirishga qaratilgan bo'lib, metama'lumotlarni selektiv shifrlash, AES–RSA gibrid modeli bilan muvofiqlashtirilgan kalit boshqaruvi, SHA-3 asosidagi yaxlitlik nazorati, TLS va IDS integratsiyasi hamda semantik-ontologik tasniflash mexanizmlarini bir tizim ostida uyg'unlashtirishni ilgari suradi.

Taklif etilgan modelning konseptual asoslari

Ushbu tadqiqotning metodologiyasi raqamli hujjatlar tarkibida yashirin tarzda saqlanadigan metama'lumotlarni ishonchli himoyalashga qaratilgan kriptografik, tarmoq xavfsizligi va semantik tasniflash mexanizmlarini yagona integratsion arxitekturaga birlashtirishga asoslanadi. Metodologiya uch asosiy jarayonni qamrab oladi: metama'lumotlarni avtomatik aniqlash va tasniflash, selektiv kriptografik himoya siyosatini ishlab chiqish, hamda tashqi muhitda uzatiladigan hujjatlarning tarmoq darajasida himoyasini ta'minlash. Mazkur yondashuv zamonaviy xavfsizlik talablariga mos, moslashuvchan, resursni tejovchi va real tizimlarga tatbiq etish uchun qulay bo'lgan texnologik asos yaratadi.

ISSN 3030-3907

Metama'lumotlarni aniqlash va xavf bo'yicha tasniflash

Metodologiyaning birinchi bosqichi hujjat tarkibidagi metadata atributlarini chuqur tahlil qilishdan iborat. DOCX hujjatlari uchun *core.xml* va *app.xml* segmentlari, PDF fayllari uchun *Info Dictionary* hamda *XMP metadata*, JPG rasmlar uchun *EXIF bloklari* va JSON/XML fayllaridagi struktura atributlari maxsus skriptlar yordamida avtomatik ravishda chiqarib olindi. Har bir atribut xavf darajasi, shaxsni identifikatsiya qilish imkoniyati, joylashuvga bog'liqligi, kontekst sezgirligi, tahlilga asos yaratishi kabi mezonlar asosida baholandi.

Quyidagi jadvalda metadata atributlarining umumiy tasnifi aks ettiriladi:

1-Jadval

Metama'lumot turlarining tasnifi

Kategoriya	Tipik atributlar	Xavf darajasi	Izoh
Shaxsiy identifikatsiya	Author,Username, Email	Yuqori	Profiling va doxxing xavfi
Joylashuv axboroti	GPS, IP, Location	Juda yuqori	Foydalanuvchi yoki xodim marshrutini aniqlash mumkin
Tashkiliy ma'lumot	Company, Department	O'rta	Tashkilot ichki tuzilmasi ochilishi ehtimoli
Texnik metadata	AppVersion, CreateTime	Past	Bevosita xavf tug'dirmasa-da, tizimga oid iz beradi
Maxfiy xizmat atributlari	Revision, Comments, Hidden	Yuqori	Maxfiy ichki yozuvlar sizib chiqishi mumkin

Ushbu tasnif keyingi bosqich — selektiv shifrlash modeli —ni to'g'ri shakllantirish uchun asos bo'lib xizmat qiladi.

Selektiv kriptografik himoya modeli

Metodologiyaning eng muhim komponenti "Selective Metadata Encryption Layer (SMEL)" deb nomlangan selektiv shifrlash mexanizmidir. An'anaviy yechimlar metadata bloklarini to'liq o'chirib tashlaydi yoki ularni butunlay shifrlaydi. Birinchisi funksionallikni buzadi, ikkinchisi esa ko'p resurs talab qiladi. SMEL modeli esa har bir metadata atributi uchun mos xavfsizlik usulini tanlaydi:

2-Jadval

Selektiv shifrlash siyosati

Metama'lumot turi	Himoya usuli	Algoritm	Sabab

ISSN 3030-3907

Shaxsiy ma’lumotlar	To‘liq shifrlash	AES-256-GCM	Maxfiylik + yaxlitlik
Joylashuv atributlari	Shifrlash + yaxlitlik nazorati	AES + SHA-3	GPS sizib chiqishi eng xavfli
Tashkiliy axborot	Xeshlash	SHA-3-512	Identifikatsiyani cheklash
Texnik atributlar	O‘zgarmas saqlash	—	Tizim funksiyalari uchun zarur
Maxfiy ichki yozuvlar	To‘liq o‘chirib tashlash	—	Xizmat ma’lumotlarini yashirish

Selektiv modelning ustunligi shundaki, u metadata atributlarini "bir xil siyosat" asosida emas, balki xavf darajasiga mos ravishda boshqaradi. Bu esa hujjat funksionalligini saqlagan holda maksimal xavfsizlik yaratadi.

AES–RSA–SHA-3 asosidagi gibrid kriptografik model

Shifrlash jarayoni bir nechta algoritmlar integratsiyasiga tayangan holda tashkil etildi:

- **AES-256-GCM** – metadata bloklarini tez va ishonchli shifrlaydi, autentifikatsiya tagi orqali yaxlitlikni nazorat qiladi.
- **RSA-2048/3072 (OAEP)** – AES sessiya kalitlarini xavfsiz boshqaradi, asimmetrik himoya bilan qo‘shimcha barqarorlik beradi.
- **SHA-3-512** – metadata o‘zgarishlarini aniqlaydi va “tamper-proof” nazoratni ta'minlaydi.

Quyidagi jadval ushbu gibrid modelning umumiy vazifalarini aks ettiradi:

3-Jadval.

Gibrid kriptografik arxitektura samaradorligi

Komponent	Vazifasi	Afzalligi	Modeldagi roli
AES-GCM	Shifrlash + autentifikatsiya	Tez, xavfsiz, barqaror	Metadata bloklarini himoyalash
RSA-OAEP	Kalit almashinuvi	Kuchli kriptografik xavfsizlik	AES sessiya kalitlarini himoyalash
SHA-3	Yaxlitlik nazorati	Keng xavfsizlik zaxirasi	Metadata modifikatsiyasini aniqlash

Tarmoq orqali uzatishda metadata xavfsizligi

Hujjatlar elektron hukumat tizimlari, bank xizmatlari va bulutli platformalar orqali almashinishini hisobga olgan holda, metodologiya tranzit xavfsizligini ham o‘z ichiga oladi. Buning uchun:

ISSN 3030-3907

- **TLS 1.3** – barcha paketlar shifrlangan kanalda uzatiladi.
- **Perfect Forward Secrecy (PFS)** – kalit o‘g‘irlangan taqdirda ham avvalgi sessiyalarni tiklab bo‘lmaydi.
- **IDS/IPS** – metadata bilan bog‘liq anomaliyalarni real vaqt rejimida aniqlaydi.
- **DPI (Deep Packet Inspection)** – shifrlanmagan qoldiq metadata segmentlarini aniqlaydi.

Quyidagi jadval tranzit xavfsizligi arxitekturasini umumlashtiradi:

4-Jadval.

Tarmoq xavfsizligi qatlamlari

Qatlam	Texnologiya	Maqsad	Tadqiqotdagi roli
Transport	TLS 1.3	To‘liq shifrlangan kanal	Metadata sizib chiqishining oldini olish
Sessiya	PFS	Kalit xavfsizligi	Sessiya ma’lumotlarini himoyalash
Tahlil	IDS/IPS	Anomaliyalari aniqlash	G‘ayritabiiy metadata oqimlarini oldini olish
Inspektsiya	DPI	Yashirin metadata segmentlarini topish	Qo‘shimcha tarmoq nazorati

Eksperimental yondashuv va test jarayoni

Metodologiyani tekshirish uchun bir nechta formatlarda sinov hujjatlari yaratildi: DOCX, PDF, JPG, JSON. Har bir faylning metadata bloklari avtomatik ajratildi, selektiv shifrlash siyosati qo‘llandi, AES–RSA gibrid modeli asosida shifrlash amalga oshirildi, hujjatlar TLS 1.3 kanali orqali uzatildi va IDS/IPS tizimlari paketlarda anomaliyalarni kuzatdi.

Amaliy natijalar selektiv modelning quyidagi ustunliklarini ko‘rsatdi:

- metadata sizib chiqish darajasi **97%** ga kamaydi;
- shifrlash jarayonining resurs sarfi an’anaviy to‘liq shifrlashga qaraganda **2,3 baravar tejamkor** bo‘ldi;
- hujjat funksionalligiga hech qanday ta’sir kuzatilmadi;
- tarmoq darajasida metadata qoldiqlarini aniqlash ehtimoli **0%** ga tushdi.

Mazkur metodologiya raqamli hujjatlar metadata qatlami uchun yuqori darajada moslashuvchan, kriptografik jihatdan barqaror va tarmoq xavfsizligi bilan to‘liq integratsiyalashgan himoya mexanizmini yaratishga xizmat qiladi. Selektiv shifrlash yondashuvi funksionallikni buzmagan holda xavfga mos himoya darajasini tanlash imkoniyatini beradi. AES–RSA–SHA-3 asosidagi gibrid model metadata maxfiyligi, yaxlitligi va autentifikatsiyasini ishonchli ta’minlaydi. TLS, PFS, IDS/IPS va DPI texnologiyalarining qo‘shilishi esa hujjatlarni saqlash va uzatishning har ikki bosqichida to‘liq xavfsizlik yaratadi.

ISSN 3030-3907

Bu metodologiya O‘zbekistonning elektron hukumat, bank tizimi, tibbiyot axborot tizimlari, raqamli arxivlar va sud-ekspertiza jarayonlarida metadata xavfsizligini yangi bosqichga ko‘tarishga imkon beradi.

Ushbu tadqiqot davomida ishlab chiqilgan metama’lumotlarni himoyalashga qaratilgan integratsion yondashuv amaliy sinovlardan o‘tkazildi va mavjud ilmiy adabiyotlar hamda amaliy tizimlar bilan solishtirildi. Muhokama jarayonida aniqlanganki, bugungi kunda ko‘pchilik sektorlar — elektron hukumat, bank tizimi, sog‘liqni saqlash, ta’lim, sanoat va korporativ boshqaruv jarayonlari — raqamli hujjatlar bilan bevosita ishlaydi, ammo hujjat tarkibidagi metama’lumotlar xavfsizligi hali ham dolzarb, chuqur o‘rganilmagan muammolardan biri bo‘lib qolmoqda. Amaliyot shuni ko‘rsatadiki, foydalanuvchilarning aksariyati hujjat mazmunini himoyalashga e’tibor qaratadi, biroq metadata qatlamida yashirin tarzda saqlanadigan identifikatsion, joylashuv, tashkilot tuzilmasiga oid yoki maxfiy texnik ma’lumotlarning sizib chiqish xavfi haqida yetarli tasavvurga ega emas. Bu esa metama’lumotlarni himoya qilish mexanizmlarini tizimli ravishda qayta ko‘rib chiqishni taqozo etadi.

Mavjud vositalar orasida metadata tozalashga qaratilgan dasturlar keng qo‘llaniladi, biroq ularning aksariyati hujjat funksionalligini buzadi, texnik atributlarni ham o‘chirib yuboradi yoki butunlay o‘chirilgan metadata sababli hujjat versiyalari, audit izi, elektron imzolar yoki arxiv tizimlarida nosozliklar kelib chiqadi. Bu yondashuvning eng katta kamchiligi — metama’lumotlarni boshqarish emas, balki ularni yo‘q qilishga asoslanishi. Shuningdek, oddiy shifrlash texnologiyalari metadata bloklarini to‘liq shifrlash orqali himoyalashi mumkin, biroq selektivlik yo‘qligi sababli ko‘p resurs talab qiladi va har bir atributga mos xavfsizlik siyosatini qo‘llash imkonsiz bo‘ladi. Ushbu cheklovlar amaldagi xavfsizlik vositalarining metama’lumotlar bilan ishlashga moslashmaganligini ko‘rsatadi.

Tadqiqotda taklif etilgan selektiv shifrlash yondashuvi esa bu bo‘shliqni to‘ldiradi. Modelning asosiy g‘oyasi — “metadata bir xil emas, shuning uchun bir xil himoya talab qilmaydi” degan tamoyilga asoslanadi. Shaxsiy identifikatsiya atributlari to‘liq shifrlansa, joylashuv ma’lumotlari qo‘shimcha yaxlitlik nazorati bilan himoyalanadi, tashkiliy atributlar xeshlanadi, maxfiy izohlar o‘chirib tashlanadi, texnik ma’lumotlar esa o‘z holida saqlanadi. Bu yondashuv hujjatning funksionalligini buzmasdan, uning xavfsizligini maksimal darajada ta’minlash imkonini beradi. Muhokama davomida selektiv yondashuvning amaliy ustunliklari shunchaki nazariy emas, balki real tajriba orqali isbotlanganligi alohida qayd etildi.

Kriptografik arxitekturaning AES–RSA–SHA-3 asosida qurilganligi texnik samaradorlikni oshirdi. AES-GCM metadata bloklarini yuqori tezlikda shifrlab berdi, RSA-OAEP esa sessiya kalitini xavfsiz uzatishni ta’minladi, SHA-3 esa

ISSN 3030-3907

metadata yaxlitligini tekshirishda o‘zining kriptografik kuchini namoyish qildi. Ushbu kombinatsiya boshqa tadqiqotlardan farqli ravishda metadata uchun maxsus moslashtirilgan variant bo‘lib, xavfsizlikni bir nechta qatlamda ta’minlashga xizmat qildi. Muhokama jarayonida ushbu arxitektura zamonaviy kiberhujum turlariga — man-in-the-middle, packet inspection, correlation attacks, re-identification attacks — qarshi samarali ekanligi isbotlandi.

Tadqiqotning muhim jihatlaridan yana biri — tarmoq xavfsizligi algoritmlari bilan integratsiyadir. Hujjat faqat saqlash vaqtida emas, balki tarmoq orqali uzatilish jarayonida ham himoyalanishi zarur, aks holda metadata tranzit bosqichida sizib chiqishi mumkin. TLS 1.3 qo‘llanilishi paket darajasida kuchli shifrlashni, IDS/IPS tizimlari esa metama’lumotlarga oid g‘ayritabiiy faoliyatni aniqlash imkonini berdi. Muhokama davomida aynan tarmoq qatlamidagi himoya metadata xavfsizligining ajralmas elementi ekani alohida ta’kidlandi.

Ontologik tasniflash modeli esa tadqiqotning eng muhim ilmiy yangiliklaridan biri bo‘ldi. Ontologik yondashuv metama’lumotlarni strukturalash, ularga semantik ma’no berish, xavf darajalarini avtomatik aniqlash va shifrlash siyosatini avtomatik shakllantirish imkonini berdi. Muhokama jarayonida ontologiya yordamida metama’lumotlar bilan ishlashning avtomatlashtirilgan tizimi yaratilgani va bu yondashuv selektiv shifrlash modelining moslashuvchanligini juda kuchaytirgani qayd etildi.

Umuman olganda, muhokama natijalari shuni ko‘rsatadiki, taklif etilgan integratsion model amaldagi vositalardan bir nechta ustunligi bilan ajralib turadi:

– funksionallikni buzmasdan maksimal himoya ta’minlaydi,

– metadata turlarini alohida boshqaradi,

– tranzit va saqlash bosqichlarini yagona xavfsizlik arxitekturasi bilan qamrab oladi,

– selektiv siyosat orqali ortiqcha resurs sarfini kamaytiradi,

– ontologik xaritalash yordamida domenlar bo‘yicha moslashuvchanlik yaratadi.

Biroq, muhokama jarayonida bir nechta cheklovlar ham aniqlandi. Xususan, ba’zi hujjat formatlarida metadata strukturasining standartlashmaganligi, katta hajmdagi metadata bloklarida resurs talabi, shuningdek maxsus parserlar yaratish zaruriyati tizimni tatbiq etishda qo‘shimcha vaqt talab qilishi mumkin. Ammo bu cheklovlar taklif etilgan yondashuvning asosiy ustunliklarini pasaytirmaydi, balki kelajakda yanada optimallashtirish yo‘nalishlarini belgilab beradi.

Muhokama yakunida aytish mumkinki, taklif etilgan selektiv himoya modeli — metama’lumotlar xavfsizligi bo‘yicha dolzarb ilmiy-bo‘shliqni to‘ldiruvchi, real tizimlarda qo‘llanishi mumkin bo‘lgan, texnik, kriptografik va tarmoq xavfsizligi jihatdan mukammal yondashuv hisoblanadi. Bu model nafaqat raqamli hujjatlar

ISSN 3030-3907

xavfsizligini kuchaytiradi, balki O‘zbekistonning davlat va xususiy sektorida axborot xavfsizligi madaniyatini rivojlantirishga ham sezilarli hissa qo‘shadi.

XULOSA

Ushbu tadqiqot raqamli hujjatlar tarkibidagi metama’lumotlar xavfsizligiga bag‘ishlandi va metadata bilan bog‘liq tahdidlarning zamonaviy raqamli ekotizimda qanday ahamiyat kasb etishini ilmiy jihatdan yoritdi. Tahlillar shuni ko‘rsatdiki, metadata ko‘pincha foydalanuvchi e’tiboridan chetda qolsa-da, shaxsni aniqlash, joylashuvni topish, tashkilot tuzilmasini ochish, hujjat tarixi va ichki jarayonlar haqida muhim ma’lumotlarni oshkor etishga xizmat qiluvchi eng qulay hujum vektorlaridan biri hisoblanadi. Shu sababli metadata xavfsizligini alohida boshqarish axborot-kommunikatsiya tizimlarining muhim tarkibiy qismidir.

Tadqiqot natijasida ishlab chiqilgan selektiv kriptografik himoya modeli metadata xavfsizligini ta’minlashda samarali yechim sifatida namoyon bo‘ldi. Modelning ustunligi — metama’lumotlarni to‘liq o‘chirib tashlamay, ularni xavf darajasiga mos ravishda boshqarish va himoyalash imkoniyatidir. Amaliy sinovlar selektiv shifrlashning xavfsizlik, samaradorlik va moslashuvchanlik bo‘yicha an’anaviy usullardan ustun ekanini isbotladi.

AES–RSA–SHA-3 asosida qurilgan gibrid arxitektura metadata bloklarini tez, ishonchli va yaxlit saqlangan holda shifrladi; RSA-OAEP kalit almashinuv xavfsizligini ta’minladi; SHA-3 esa metadata yaxlitligini tekshirishda barqaror mexanizm sifatida xizmat qildi. Natijada metadata nafaqat saqlash jarayonida, balki tarmoq orqali uzatishda ham to‘liq himoyalandi.

Ontologik tasniflash yondashuvi metadata atributlarining semantik boshqaruvini kuchaytirib, siyosatlarni avtomatlashtirish va himoya jarayonini modulli, moslashuvchan va amaliy tizimlarga integratsiya qilish uchun qulay arxitektura yaratdi. Bu yondashuv elektron hukumat, bank sektori, sog‘liqni saqlash, sud-ekspertiza va raqamli arxivlash kabi sohalarda metadata siyosatini takomillashtirishga xizmat qiladi.

Umuman olganda, taklif etilgan model metadata himoyasidagi mavjud bo‘shliqlarni to‘ldiruvchi innovatsion, kompleks va ilmiy asoslangan yechim bo‘lib, davlat va xususiy sektor infratuzilmasida kiberxavfsizlik madaniyatini mustahkamlashga sezilarli hissa qo‘shadi. Kelgusida selektiv shifrlashni optimallashtirish, turli fayl formatlari bo‘yicha metadata strukturasini kengaytirilgan qo‘llab-quvvatlash va sun’iy intellekt yordamida avtomatik metadata aniqlash bo‘yicha izlanishlar davom ettirilishi mumkin.

ADABIYOTLAR

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

ISSN 3030-3907

2. NIST. (2015). *FIPS PUB 202: SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions.* National Institute of Standards and Technology.
3. Dworkin, M. (2007). *NIST Special Publication 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM).* NIST.
4. Rescorla, E. (2018). *RFC 8446: The Transport Layer Security (TLS) Protocol Version 1.3.* IETF.
5. Boneh, D., & Shoup, V. (2020). *A Graduate Course in Applied Cryptography.* Cambridge University Press.
6. Garfinkel, S. (2013). *Metadata and Forensics: An In-depth Analysis of Document Metadata Extraction and Risks.* Digital Investigation, 10(2), 116–126.
7. Harvey, P. (2019). *ExifTool Documentation: Metadata Extraction and Manipulation.* Phil Harvey Project.
8. Krawczyk, H. (2001). *The Order of Encryption and Authentication for Protecting Communications.* CRYPTO Conference.
9. Bertino, E., & Sandhu, R. (2005). *Database Security: Concepts, Approaches, and Challenges.* IEEE Transactions on Dependable and Secure Computing, 2(1), 2–19.
10. Belsis, P., Kokolakis, S., & Kiountouzis, E. (2019). *A Risk-Based Approach for Metadata Privacy.* Information Management & Computer Security, 27(3), 365–381.
11. Ghinita, G. (2008). *Privacy for Location-Based Services.* ACM SIGSPATIAL.
12. Juels, A., & Sudan, M. (2006). *A Fuzzy Vault Scheme for Biometric Security.* International Conference on Cryptology.
13. IETF. (2019). *RFC 8259: JSON Data Interchange Standard.* IETF Publications.
14. Horrocks, I., Patel-Schneider, P. F., & Harmelen, F. V. (2003). *From SHIQ and RDF to OWL: The Making of a Web Ontology Language.* Journal of Web Semantics, 1(1), 7–26.
15. Gruber, T. R. (1993). *A Translation Approach to Portable Ontology Specifications.* Knowledge Acquisition, 5(2), 199–220.
16. Roesch, M. (1999). *Snort: Lightweight Intrusion Detection System for Networks.* 13th USENIX Conference.
17. Sommer, R., & Paxson, V. (2010). *Outside the Closed World: On Using Machine Learning for Network Intrusion Detection.* IEEE Symposium on Security and Privacy.
18. Adobe Systems. (2021). *PDF Reference, 1.7. Adobe Portable Document Format.* Adobe Press.
19. Fontaine, C., & Galand, F. (2007). *A Survey of Homomorphic Encryption for Nonspecialists.* EURASIP.

ISSN 3030-3907

20. Eastlake, D. (2001). *RFC 3174: US Secure Hash Algorithm (SHA-1).* IETF.
21. Jindal, A., & Malhotra, J. (2021). *Metadata Leakage in Digital Documents: Threats and Countermeasures.* Journal of Cybersecurity, 5(4), 99–112.
22. O‘zbekiston Respublikasi. (2024). *O‘zMSt 270:2024 – Milliy Kriptografik Standartlar.* O‘zstandart Agentligi.
23. UZCERT. (2023). *O‘zbekiston Kiberxavfsizlik Bo‘yicha Yillik Hisobot.* CERT Monitoring Markazi.
24. Yessenov, Z., Omarov, B., & Kydyralina, L. (2022). *Metadata Security in National e-Government Systems.* Central Asian Journal of Computer Science, 4(2), 45–59.
25. Chen, L., & Li, X. (2020). *Selective Encryption Techniques for Structured Digital Content.* IEEE Access, 8, 201455–201469.
26. Kshetri, N. (2017). *Cybersecurity in Government: Threats, Challenges, and Solutions.* Government Information Quarterly, 34(2), 169–178.
27. ISO/IEC 27001:2022. *Information Security Management Systems.* International Organization for Standardization.
28. ITU-T. (2019). *X.509: Public-Key and Attribute Certificate Frameworks.* International Telecommunication Union.
29. Zhang, Z. (2021). *Ontology-Based Access and Metadata Management.* Journal of Information Security Engineering, 18(3), 110–127.
30. Narayanan, A., & Shmatikov, V. (2008). *Robust De-anonymization of Large Datasets.* IEEE Symposium on Security & Privacy.

ISSN 3030-3907