AXBOROT KOMMUNIKATSIYA TIZIMLARIDA OPERATSION TIZIMNI XAVFSIZ YUKLAB OLISH VA TEKSHIRISH USULI

Saparova G.A

Nukus davlat texnika universiteti, Sun'iy intellekt va kiberxavfsizlik kafedrasi assistenti.

CA tomonidan berilgan sertifikat foydalanuvchining ochiq kaliti va ushbu foydalanuvchini identifikatsiya qiluvchi ma'lumotlarini, shuningdek, boshqa xizmat ma'lumotlarini o‘z ichiga oladi. Ochiq kalit sertifikatlarini yaratish bilan bir qatorda, CA ning asosiy vazifalari foydalanuvchilarni aniqlash, sertifikatlarni bekor qilish, CRL ni (certificate revocation list, bekor qilingan sertifikatlar ro‘yxati) yaratish va yangilash vazifalarini o‘z ichiga oladi.

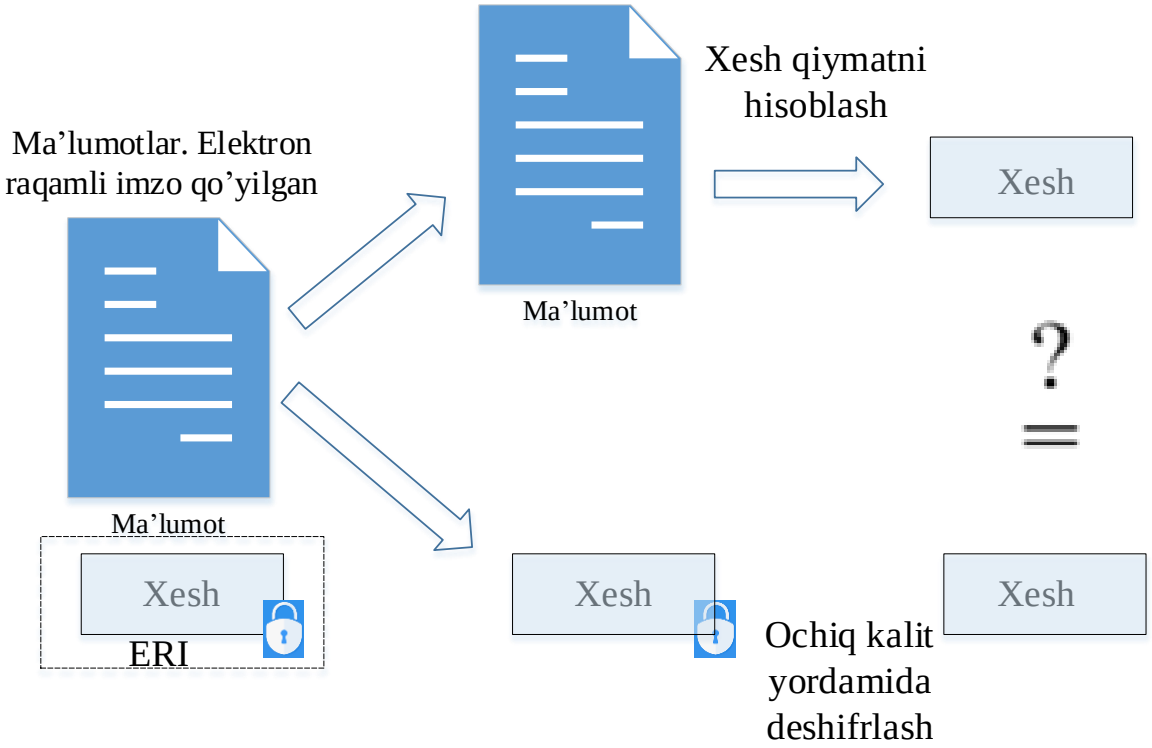
CA funksiyalarini bajaradigan server qat'iy ravishda tashkilotning nazorat qilinadigan hududida joylashgan bo‘lishi va tashqi ulanishlarga ega bo‘lmasligi yoki tarmoqdan butunlay uzilgan bo‘lishi kerak. Bunday holda, tizimning barcha foydalanuvchilari uchun real vaqt rejimida berilgan sertifikat holatini (yaroqli yoki bekor qilingan) tekshirish imkonini beruvchi resurs mavjud bo‘lishi kerak. Qoidaga ko‘ra, bunday resurs sifatida ma'mur tomonidan doimiy yangilanib turiladigan bekor qilingan sertifikatlar ro‘yxatini (CRL) o‘z ichiga olgan server yoki sertifikatlar maqomini onlayn tekshiradigan xizmat mavjud server (Online Cerfticate Status Protocol - OCSP) foydalaniladi. Ikkinchi holda sertifikat maqomi to‘g‘risidagi axborot ahamiyatliroq hisoblanadi, chunki mazkur xizmat axborotni to‘g‘ridan-to‘g‘ri CA reestridan oladi hamda bunday xizmatning javobi cheklangan bo‘ladi va javob yetarlicha katta hajmli bo‘lgan CRL bilan solishtirganda juda kichik bo‘ladi. Biroq bu holda CA serveri onlayn rejimda bo‘lishi lozim va o‘z bazasida OCSP xizmatiga murojat qilish imkoniyatini taqdim etishi lozim, bu esa barcha beriladigan sertifikat imzolanadigan CA kalitini kompramentatsiyasi va ruxsatsiz foydalanilishi tahdidini paydo qiladi. Bu holda tasdiqlovchi markazlar shajarali arxitekturasini takomillashtirish nazarda tutiladi, ya'ni, tashkilot tarmog‘iga ulaMagan ildizli va o‘z bazasiga OCSP xizmatini ulash imkoniyatini beradigan hamda foydalanuvchilarga sertifikat taqdim etadigan markaz.

Ishlab chiqilayotgan yechimda terminal serveri ikkita kalitlarga ega: yopiq va ochiq, ochiq kalitga egalik fakti va ushbu ochiq kalitning yopiq kalit bilan bog‘langanligi CA tomonidan berilgan sertifikat bilan tasdiqlangan.

OT obrazini uzatishda server uni yopiq kaliti bilan imzolaydi. Amaldagi elektron imzo algoritmida bosqichlardan biri sifatida xesh funksiyasi ham qo‘llaniladi: imzo funksiyasining kiritilishi tasvirning o‘zi emas, balki uning xesh qiymati hisoblanadi. Ammo bu usul va oddiy xeshlash usuli o‘rtasidagi asosiy farq shundaki, OT uchun hisoblangan xesh qiymati tokenda doimiy saqlaMaydi va agar OT o‘zgarsa, vaqti-vaqti bilan yangilanib turish kerak emas. Qabul qilingan obrazdan har safar mijozda hisoblab chiqiladi va ochiq kalit serveri yordamida elektron imzoning shifrini ochish natijasi bilan taqqoslanadi. Ushbu jarayon 3.2-rasmda keltirilgan.

Shunday qilib, agar administrator yuklab olingan obrazga o‘zgartirishlar kiritgan bo‘lsa (o‘rnatilgan dasturiy ta’minot yoki yangilanishlar), bu skanerlashning muvaffaqiyatiga ta’sir qilmaydi.

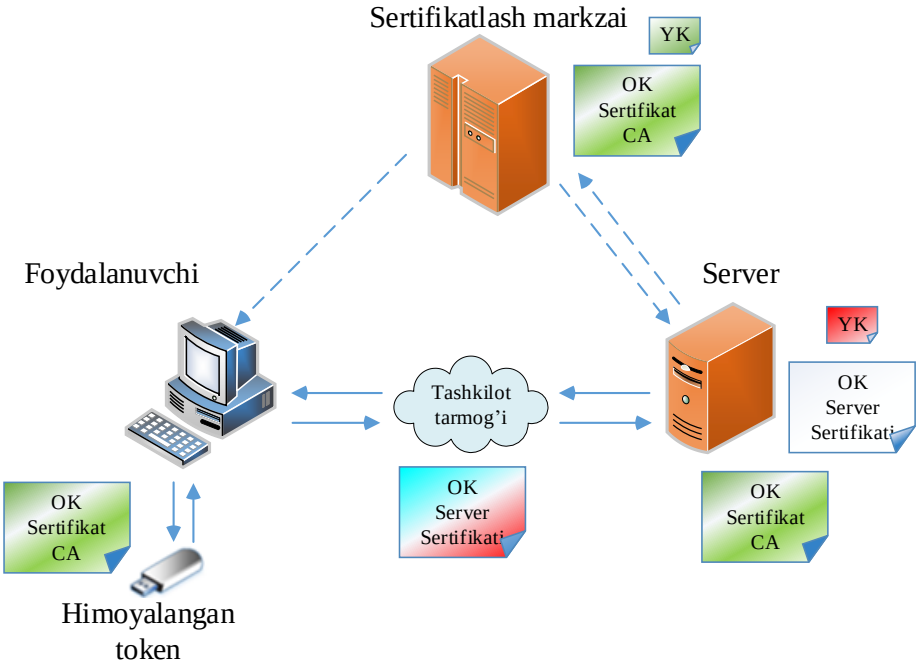
OT obrazini yuklash va yaxlitligini tekshirish usulini amalga oshirish. Uzatilayotgan obrazning yaxlitligini monitoring qilishning ishlab chiqilgan usulini amalga oshirish server tomonida obrazning elektron imzosini shakllantirishni va tasvirning o‘zini, imzo va ochiq kalit sertifikatini tekshirish uchun mijozga o‘tkazishni o‘z ichiga oladi. 3.3-rasmda Elektron imzoni tekshirish mexanizmi keltirib o‘tilgan.



3.3-rasm. Elektron imzoni tekshirish mexanizmi

Ammo bu holatda Man-in-the-middle hujumi xavfi mavjud: buzg‘unchi uzatilgan tasvirni ushlab, kaliti bilan imzolashi va sertifikatini mijozga o‘tkazishi mumkin. Ushbu tahdidni zararsizlantirish uchun CA ochiq kalit sertifikatini (yoki ierarxik CA tuzilmasida sertifikatlar zanjiri) tashqi kalit tashuvchida saqlash taklif etiladi. Server uchun ochiq kalit sertifikatini yaratishda CA berilgan sertifikatni yopiq kaliti bilan tekshiradi, bu esa uzatilgan obrazning elektron imzosini tekshirish vaqtida server sertifikatining haqiqiyligini tekshirish imkonini beradi. Shunday qilib, taklif qilingan yechimni amalga oshirish uchun zarur bo‘lgan PKI tarkibiga kiritilgan komponentlar 3.4-rasmda keltirilgan.

Elektron raqamli imzoni tekshirish uchun birinchi bosqichda OT obrazining xesh funktsiyasi qiymati hisoblab chiqiladi va ikkinchi bosqichda elektron imzo algoritmi tomonidan taqdim etilgan to‘g‘ridan-to‘g‘ri matematik o‘zgarishlar amalga oshiriladi, bu esa barcha uchta komponentni tekshirishni nazarda tutadi: xesh funktsiyasi, elektron imzo va imzolovchining ochiq kaliti[10]. Agar tekshirish natijasi ijobiy bo‘lsa, elektron imzo to‘g‘ri deb hisoblanadi va natijada olingan obraz haqiqiy hisoblanadi. Aks holda, OT tasviriga o‘zgartirishlar kiritilgan deb hisoblanadi.



3.4-rasm. Kompyuterda OT obrazining yaxlitligini tekshirish va yuklashning ishlab chiqilgan usuli uchun PKI komponentlari.

Usulga jalb qilingan PKI komponentlari:

- CA - sertifikatlashtirish markazi;
- M - mijoz:
- TS - terminal serveri;
- k_s serverining yopiq kaliti;
- k_0 - server ochiq kalit sertifikati;
- k_{CA} - sertifikatlashtirish markazining ochiq kalit sertifikati;
- OT - operatsion tizimining obrazi;
- h - hesh funksiyasi;
- f - elektron imzoni hisoblash funksiyasi;
- v - elektron imzoni tekshirish funksiyasi.

OT obrazining butunligini yuklab olish va tekshirish usuli:

1-qadam. Token TS mijoziga ulangandan so‘ng TS terminal serveridan OT obrazini yuklash protokolini ishga tushirish.

2-qadam. OT obrazini va server uchun ochiq kalit sertifikatini olish uchun transport vositasiga so‘rovni shakllantirish.

3-qadam. Server tomonida obrazning elektron imzosini shakllantirish: $f(h(OT), k_s)$, bu yerda h(OT) OT obrazining xesh funksiyasi.

4-qadam. Serverning k_0 sertifikatini, serverning shaxsiy kaliti k_s bilan imzolangan OT obrazini olish.

5-qadam. Obrazning yaxlitligini va imzoning haqiqiyligini tekshirish: $v(h(OT), k_0)$.

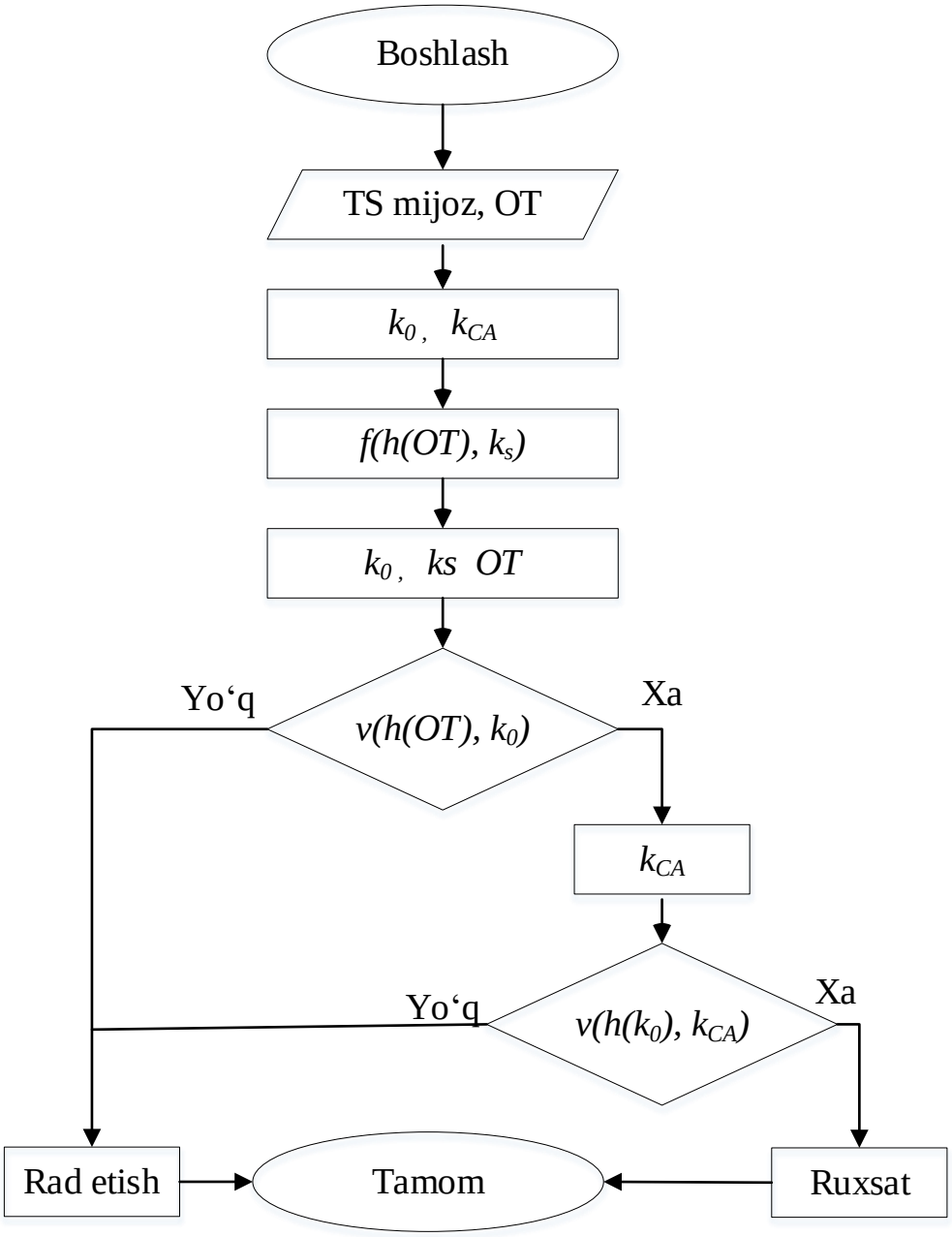
6-qadam. k_{CA} ildiz sertifikati uchun tokenga murojaat qilish.

7-qadam. Server ochiq kalit sertifikatining haqiqiyligini tekshirish: $v(h(k_0), k_{CA})$.

8-qadam. Ikkala tekshiruv ham muvaffaqiyatli bo‘lsa, OT obrazi RAM xotirasiga yuklanadi va boshqaruv unga o‘tkaziladi.

Ishlab chiqilayotgan yechimning funksionalligi uchun yana bir muhim talab - barcha ishtirok etuvchi komponentlarning ishonchli autentifikatsiyasi: server, mijoz, token va foydalanuvchi.

OTda foydalanuvchini keyingi autentifikatsiya qilish jarayoni, shuningdek, himoya darajasini oshirishni talab qiladigan jarayonlar doirasida taqdim etilgan maxsus operatsiyalarni bajarish ushbu yechimning majburiy bosqichi ekanligini tushunish kerak. Foydalanuvchiga qo‘shimcha sirlarni saqlash uchun talablarni qo‘shish uning ishini murakkablashtirganiga qaramay, muqobil variant (to‘ldirilgan avtorizatsiya bilan OT tasvirini uzatish) ma’lumotlarga ruxsatsiz kirish uchun katta xavf tug‘diradi. 3.5-rasmda OT obrazining butunligini yuklab olish algoritmining blok sxemasi tasvirlangan.



3.5-rasm. OT obrazining butunligini yuklab olish algoritmining blok sxemasi.

Taklif etilayotgan usulni mavjud yaxlitlik monitoringi usullari bilan solishtirish va tahlil qilish. Kompyuterga OTning yaxlitligini tekshirish va yuklashning ishlab chiqilgan

usulini muqobil usullar bilan solishtirish uchun ushbu usullar asosida tuzilgan algoritmlarning rasmiy me'zonlarini aniqlash kerak. Ishga ko'ra, yaxlitlikni nazorat qilish algoritmlarining xavfsizligini baholash ushbu algoritmlarning asosiy me'zonlari tomonidan ma'lum bir ehtimollik bilan himoyalangan ma'lumotlardan ruxsatsiz foydalanishni (yaxlitlikni buzish) rad etishni ta'minlash qobiliyati orqali aniqlanishi mumkin.

Butunlikni monitoring qilish algoritmlari me'zonlarini tahlil qilish asosida quyidagi ehtimolliklar aniqlanadi:

R_{RF}^{a} - algoritmning o'ziga (matematik transformatsiya yoki kriptografik ibtidoiy) muvaffaqiyatli hujum qilish (RF) ehtimoli;

R_{RF}^{l} - mahalliy saqlangan boshqaruv qiymatlarining buzilishi tufayli muvaffaqiyatsiz RF ehtimoli;

R_{RF}^{k} - asosiy ma'lumotlarning buzilishi tufayli RF ehtimoli.

Tizimdagi TS larning ishlash shartlari har xil bo'lgani va ular bilan ishlaydigan foydalanuvchilarga, joylashuvga, ko'rilgan tashkiliy chora-tadbirlarga va hokazolarga bog'liq bo'lganligi sababli, asosiy ma'lumotlarga va mahalliy saqlanadigan boshqaruv qiymatlariga hujumlar turli M lar uchun har xil muvaffaqiyat ehtimoliga ega. Shu bilan birga, RF ni himoyalangan ma'lumotlarga tatbiq etish, hech bo'lmaganda M lardan birida himoya mexanizmi to'g'ri ishlamaganligini anglatadi. Keyin mahalliy saqlangan boshqaruv qiymatlarining buzilishi tufayli ruxsatsiz foydalanish ehtimoli quyidagicha aniqlanadi.

$$R_{RF}^{k} = 1 - \prod_{i=1}^{n} R_{i}^{k},$$

bu yerda, R_{i}^{k} - i- mijoz uchun asosiy axborotni himoyalash mexanizmlarini togri ishlash ehtimolligi.

Shunday qilib, himoyalangan ma'lumotlarga RF ehtimolligi quyidagicha aniqlanadi:

$$R_{RF} = R_{RF}^{a} \times \left(1 - \prod_{i=1}^{n} R_{i}^{l}\right) \times \left(1 - \prod_{i=1}^{n} R_{i}^{k}\right).$$

Bunda butunlilikni nazoratlash algoritmlarini himoyalanganligini baholash:

$$R_{HIMOYA} = R_{HIMOYA}^{a} \times R_{HIMOYA}^{l} \times R_{HIMOYA}^{k} = (1 - R_{RF}^{a}) \times (\prod_{i=1}^{n} R_{i}^{l}) \times \prod_{i=1}^{n} R_{i}^{k}$$

.

Algoritmlarning xavfsizlik ko'rsatkichlarining qiyosiy tahlilini o'tkaziladi:

1. Siklik ortiqcha kodni hisoblashga asoslangan algoritmlar (nazorat summalari).
2. Kalitsiz xesh funksiyalarni hisoblashga asoslangan algoritmlar.
3. Asosiy xesh-funksiyalarni hisoblash asosidagi algoritmlar.
4. PKI (ERI hisoblari) asosidagi algoritmlar.

$R_{HIMOYA}^{a}, R_{HIMOYA}^{l}, R_{HIMOYA}^{k}$ himoyalanganlik ko'rsatkichlarini baholash quyidagi jadvalda ko'rsatilgan:

3.1-jadval. Yaxlitlikni monitoring qilish algoritmlarida ruxsatsiz foydalanishga qarshi xavfsizlik ko'rsatkichlari qiymatlarining qiyosiy tahlili

Algoritm / Ko'rsatkich	Nazorat summalari (NS)	Kalitsiz xesh-funksiya (KXF)	Kalitli xesh funksiyalar (XF)	Elektron raqamli imzo (ERI)

R^{a}_{HIMOYA}	Past	O‘rta	Yuqori	Yuqori
R^{l}_{HIMOYA}	Past	Past	1	1
R^{k}_{HIMOYA}	1	1	O‘rta	Yuqori

Kriptotahlil natijalari asosida eng mashhur algoritmlarning har bir guruhidan (CRC32, MD5, SHA2, SHA3, ГОСТ Р 34.11-2012, MAS, imitativ kiritish rejimida O‘z Dst 1105:2009, ECDSA, RSA) kolliziyani yoki obrazni topish bo‘yicha nazorat summasini hisoblash algoritmlari eng past murakkabligiga ega. Uzoq vaqt davomida kriptoanalitiklarning diqqat markazida bo‘lgan kalitsiz xesh-funksiya algoritmlari uchun (MD5, SHA2), bunday hujumlarning murakkabligi 2^{37} dan 2^{39} tagacha xesh operatsiyalari oralig‘ida bo‘ladi. Ammo asosiy xesh funktsiyalari va elektron raqamli imzo algoritmlariga kelsak, xavfsizlik ko‘rsatkichi ancha yuqori, chunki shifrlash algoritmlarining kuchi ishlatiladigan xesh funksiyalarining kriptografik kuchiga ham qo‘shiladi.

ERI va kalit xesh-funksiya algoritmlarida mahalliy saqlangan boshqaruv qiymatlarining buzilishi natijasida algoritmlarni buzishdan himoya qilish parametri uchun bu ehtimollik 1 ga teng, chunki bunday saqlash algoritm mantig‘ida ko‘zda tutilmagan. Aksincha, nazorat summalari va kalitsiz xesh funksiyalari uchun mijoz tomonidan tekshirish qiymatlariga ega bo‘lish (va muntazam ravishda yangilash) zarurati ularning himoyalanganlik ko‘rsatkichini sezilarli darajada kamaytiradi. Ushbu algoritmlarda kalit qiymatlarning yo‘qligi asosiy xesh-funksiyalar va ERI algoritmlaridan farqli o‘laroq, ularga ruxsatsiz kirish ehtimolini 0 ga teng deb tan olish imkonini beradi (butun tizimni buzadigan simmetrik kalit o‘zgarishi sababli simmetrik kalitni saqlash zarurati) (ishlatiladigan PKI tizimning boshqa barcha komponentlarini bittasi buzilgan taqdirda himoya qilishga imkon beradi, ammo shaxsiy kalitlarning xavfsizligi hali ham yuqori darajada saqlanishi kerak).

Shunday qilib, berilgan yaxlitlik monitoringi algoritmlarini taqqoslash asosida quyidagi munosabatlarni shakllantirish mumkin:

$$R_{HIMOYA_{NS}} < R_{HIMOYA\_KHF} < R_{HIMOYA\_HF} < R_{HIMOYA\_ERI}$$

Natijada, mijozga OT yaxlitligini tekshirish va yuklash usulini amalga oshirishda foydalaniladigan ERI asosida yaxlitlilikni nazoratlash algoritmi RF dan himoyalanganlik ko‘rsatkichi yuqori emas degan xulosaga kelsih mumkin.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI:

1.Гатчан, Ю.А., Теплоухова, О.А. Способы контроля целостности образа операционной системы при удаленной загрузке на тонкие клиенты в системах терминального доступа. Электронный сборник тезисов докладов II Всероссийского конгресса молодых ученых, СПбНИУ ИТМО (Санкт-Петербург, апрель 2013). - 2013. - С. 52-53.

2.Левоневский Д.К., Ватаманюк И.В, Малов Д.А. Обеспечение доступности сер висов корпоративного интеллектуального пространства посредством управле ния потоком входных данных. Программная

инженерия, т. 10, № 1, 2019. С. 20 29. DOI: 10.17587/prin.10.20-29

3.Осипов В.Ю., Воробьев В.И., Левоневский Д.К. Проблемы защиты от ложной информации в компьютерных сетях. Труды СПИИРАН. 2017. № 53. С. 97-117. DOI: 10.15622/sp.53.5

4.Levonevskiy, D., Vatamaniuk, I., Saveliev, A. Processing models for conflicting user requests in ubiquitous corporate smart spaces. MATEC Web of Conferences, 161, 3006, 2019. DOI: 10.1051/matecconf/201816103006

5.Bhardwaj, M.D. Alshehri, K. Kaushik, H.J. Alyamani, M. Kumar "Secure framework against cyber-attacks on cyber-physical robotic systems" Journal of Electronic Imaging, 2022

6.K. Millar, A. Cheng, H.G. Chew, C.C. Lim "Operating system classification: a minimalist approach" 2020 International Conference on Machine Learning and Cybernetics (ICMLC) (2020), pp. 143-150

7.S. Peng, A. Zhou, S. Liao, L. Liu "A threat actions extraction method based on the conditional co-occurrence degree" 7th International Conference on Information Science and Control Engineering (ICISCE) (2020), pp. 1633-1637

8.Powell, M., Brule, J., Pease, M., Stouffer, K., Tang, C., Zimmerman, T., Deane, C., Hoyt, J., Raguso, M., Sherule, A. & Zheng, K., (2022). Protecting information and system integrity in industrial control system environments.

9.Murthy, S., Bakar, A. A., Rahim, F. A., & Ramli, R. (2019, May). A comparative study of data anonymization techniques. In 2019 IEEE 5th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS) (pp. 306–309). IEEE.