VETERINARIYA AVTOMATLASHTIRILGAN AXBOROT TIZIMIDA (VAAT) AXBOROT XAVFSIZLIGINI TA‘MINLASH ARXITEKTURASI

Rustamova Moxichexra Yaxshiboyevna
Muhammad al-Xorazmiy nomidagi TATU, o‘qituvchi
mohimrustamova83@gmail.com
Abilov Dilshod Bekzod o‘g‘li
Muhammad al-Xorazmiy nomidagi TATU, talaba abilovdilshod55@gmail.com

Annotatsiya: *Ushbu maqolada Veterinariya avtomatlashtirilgan axborot tizimi (VAAT) doirasida axborot xavfsizligini ta’minlashning to‘rt bosqichli arxitekturasi tahlil qilinadi. Tadqiqot natijasida foydalanuvchini autentifikatsiya qilish (OneID), formatli xatoliklarni karrali nazorat orqali filtrlash, barcha harakatlarni LOG va Audit jurnalida qayd etish hamda ma’lumotlarni PostgreSQL va kesh xotira asosida boshqarish mexanizmlarining uzviy bog‘langan holda ishlashi asoslab berildi. Tavsiya etilgan arxitektura tizimga faqat tekshiruvdan o‘tgan qonuniy so‘rovlarning kirishini, sodir bo‘lgan har bir amalning esa izlanadigan bo‘lib qayd etilib borishini ta’minlaydi. Modelning amaliy qo‘llanilishi veterinariya sohasida elektron xizmatlarni ko‘rsatishda axborotning yaxlitligi, maxfiyligi va foydalanish qulayligini bir vaqtning o‘zida ta’minlashga xizmat qiladi.*

Kalit so‘zlar: *veterinariya axborot tizimi, VAAT, axborot xavfsizligi, autentifikatsiya, OneID, karrali nazorat, LOG jurnal, audit jurnal, PostgreSQL, Yagona darcha, singlewindow.uz.*

АРХИТЕКТУРА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ ВЕТЕРИНАРИИ (АИСВ)

Рустамова Мохичехра Яхшибоевна
Ташкентский университет информационных технологий имени Мухаммада аль-Хорезми, преподаватель E-mail: mohimrustamova83@gmail.com
Абилов Дилшод Бекзод угли
Ташкентский университет информационных технологий имени Мухаммада аль-Хорезми, студент E-mail: abilovdilshod55@gmail.com

Аннотация: *В статье анализируется четырёхуровневая архитектура обеспечения информационной безопасности в рамках Автоматизированной информационной системы ветеринарии (АИСВ). В результате исследования обоснована взаимосвязанная работа механизмов аутентификации пользователя (OneID), фильтрации ошибок формата через многократный контроль, регистрации всех действий в LOG и аудит-журнале, а также управления данными на основе PostgreSQL и кэш-памяти. Предложенная архитектура обеспечивает*

поступление в систему только проверенных законных запросов и отслеживаемую регистрацию каждой операции.

Ключевые слова: *ветеринарная информационная система, АИСВ, информационная безопасность, аутентификация, OneID, многократный контроль, LOG-журнал, аудит-журнал, PostgreSQL, Единое окно.*

INFORMATION SECURITY ARCHITECTURE IN THE VETERINARY AUTOMATED INFORMATION SYSTEM (VAIS)

Rustamova Moxichexra Yaxshiboyevna
Lecturer, Tashkent University of Information Technologies named after Muhammad al-Khwarizmi E-mail: mohimrustamova83@gmail.com
Abilov Dilshod Bekzod o‘g‘li
Student, Tashkent University of Information Technologies named after Muhammad al-Khwarizmi E-mail: abilovdilshod55@gmail.com

Abstract: *This article analyzes a four-layer information security architecture within the Veterinary Automated Information System (VAIS). The research substantiates the interconnected functioning of user authentication mechanisms (OneID), format error filtering through multi-level control, registration of all actions in LOG and audit journals, as well as data management based on PostgreSQL and cache memory. The proposed architecture ensures that only verified legitimate requests enter the system and that every operation is registered in a traceable manner.*

Keywords: *veterinary information system, VAIS, information security, authentication, OneID, multi-level control, LOG journal, audit journal, PostgreSQL, Single Window.*

KIRISH

Zamonaviy davlat boshqaruvi sohasida raqamli xizmatlarning tez sur’atlar bilan rivojlanishi axborot tizimlarining xavfsizligini ta’minlash masalasini birinchi darajali dolzarblikka aylantirmoqda. Veterinariya sohasidagi elektron xizmatlar - jumladan, chegara veterinariya nazorati, elektron sertifikatlash va laboratoriya tekshiruvlari natijalarini raqamli shaklda uzatish - tashqi savdo ishtirokchilari, davlat organlari va fuqarolar o‘rtasidagi ma’lumot almashinuvining xavfsiz va ishonchli bo‘lishini talab qiladi.

Veterinariya avtomatlashtirilgan axborot tizimi (VAAT) - chegara veterinariya nazorati va tashqi savdodagi veterinariya operatsiyalarini raqamlashtirishga qaratilgan zamonaviy platforma bo‘lib, uning samaradorligi ma’lumotlarning yaxlitligi (integrity), maxfiyligi (confidentiality) va foydalanish qulayligi (availability) tamoyillari - ya’ni CIA-triadasining birgalikda ta’minlanishiga bevosita bog‘liq. Mazkur talablar ISO/IEC 27001:2022 axborot xavfsizligi boshqaruvi tizimlariga qo‘yiladigan xalqaro standartda ham rasman belgilangan.

Ushbu maqolaning maqsadi -VAAT tizimida foydalanuvchi arizasining kirish nuqtasidan boshlab yakuniy saqlash bosqichigacha bo‘lgan barcha oqim davomida axborot xavfsizligini ta’minlashning to‘rt qatlamli arxitekturasini tahlil qilish va uning ilmiy-amaliy asoslarini ochib berishdir. Maqolada har bir qatlamning texnik va institutsional funksiyasi, qatlamlar orasidagi o‘zaro bog‘liqlik hamda arxitekturaning umumiy samaradorligi yoritiladi.

Adabiyotlar tahlili va muammoning qo‘yilishi

Axborot xavfsizligini ta’minlash sohasidagi ilmiy tadqiqotlar so‘nggi yillarda ko‘p qatlamli himoya modellari (defense-in-depth) va nol ishonch (zero-trust) arxitekturasiga alohida e’tibor qaratmoqda. Smith va boshqalar (2021) davlat axborot tizimlarida ko‘p qatlamli autentifikatsiya mexanizmlarining ma’lumot yaxlitligiga ijobiy ta’sirini isbotlaganlar. Lee, Park va Kim (2022) esa formatli va mantiqiy nazoratni birlashtirgan karrali validatsiya modellarining samaradorligini ilmiy jihatdan asoslaganlar.

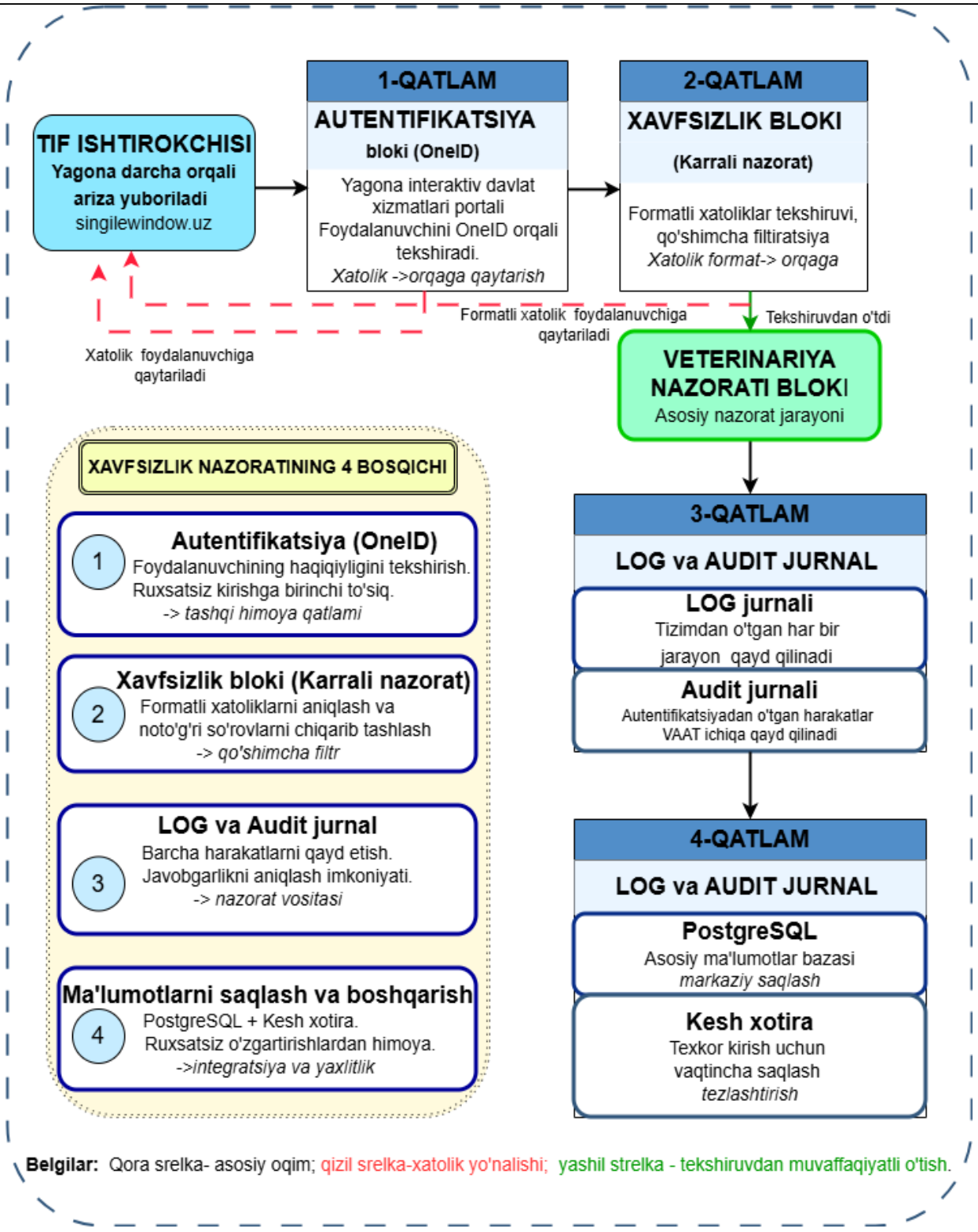
Elektron davlat xizmatlarining barqarorligi va ishonchliligi kontekstida Brown (2023) audit jurnallarini yuritish orqali javobgarlikni ta’minlashning muhim ahamiyatini qayd etgan. Shu bilan birga, veterinariya sohasidagi maxsus axborot tizimlarida xavfsizlik arxitekturasini kompleks yondashuv asosida tahlil qiluvchi tadqiqotlar hozircha yetarli darajada rivojlanmagan. Mazkur maqolada aynan shu bo‘shliqni to‘ldirish, ya’ni VAAT misolida veterinariya sohasi uchun moslashtirilgan axborot xavfsizligi arxitekturasini taklif etish maqsad qilingan.

Tadqiqot usullari

Tadqiqotda tizimli tahlil (system analysis), qatlamli modellashtirish (layered modeling) va arxitektura shakllantirish (architecture design) usullaridan foydalanildi. Modellashtirish jarayonida ISO/IEC 27001:2022 xalqaro standarti, OWASP tavsiyalari va O‘zbekiston Respublikasi Davlat standarti (O‘z DSt 2590:2012- Axborot tizimlari interoperabelligi) talablariga tayanildi. Arxitektura komponentlari bosqichma-bosqich, ma’lumot oqimining kirish nuqtasidan yakuniy saqlash bo‘g‘inigacha bo‘lgan zanjir bo‘ylab tahlil qilindi.

Natijalar va muhokama

VAAT tizimida axborot xavfsizligi foydalanuvchi Yagona darcha (singlewindow.uz) orqali ariza yuborgan dastlabki bosqichdanoq nazorat ostiga olinadi. Tadqiqot natijalari shuni ko‘rsatdiki, tizim to‘rt bosqichli xavfsizlik nazorat zanjiri asosida ishlaydi va uning umumiy arxitekturasi 1-rasmda keltirilgan.



1-rasm. VAAT tizimida axborot xavfsizligini ta’minlash arxitekturasi (to‘rt bosqichli nazorat zanjiri)

Birinchi qatlam -Autentifikatsiya bloki

Ariza Yagona interaktiv davlat xizmatlari portali (OneID) orqali o‘tkazilib, undan so‘ng Autentifikatsiya bloki orqali foydalanuvchining haqiqiyligi tekshiriladi. OneID - O‘zbekiston Respublikasida shakllangan yagona identifikatsiya tizimi bo‘lib, u foydalanuvchini turli davlat xizmatlarida bir marta ro‘yxatdan o‘tgan hisob orqali tanib olish imkonini beradi. Agar autentifikatsiya yoki avtorizatsiyada xatolik aniqlansa, tizim darhol xatolik haqida xabar berib, foydalanuvchini yana Yagona darchaga yo‘naltiradi.

Bu ruxsatsiz yoki noto‘g‘ri kirish urinishlarining tizim ichkarisiga o‘tishiga yo‘l qo‘ymaydigan birinchi himoya qatlamini tashkil etadi.

Ikkinchi qatlam- Xavfsizlik bloki (Karrali nazorat)

Autentifikatsiyadan muvaffaqiyatli o‘tgan so‘rov keyingi bosqichda Xavfsizlik bloki - Karrali nazorat orqali tekshiriladi. Ushbu blok formatli xatoliklar mavjudligini aniqlaydi: majburiy maydonlarning to‘liqligi, ma’lumotlar formatining muvofiqligi, sintaktik xatoliklar va kirituv chegaralari tekshiriladi. Agar formatli xatolik topilsa, jarayon yana orqaga qaytariladi. Xatolik aniqlanmagan taqdirdagina ariza keyingi Veterinariya nazorati blokiga o‘tkaziladi. Shu tariqa Karrali nazorat tizimga faqat to‘g‘ri formatlashtirilgan, tekshiruvdan o‘tgan ma’lumotlarning kirishini ta’minlovchi qo‘shimcha filtr vazifasini bajaradi.

Uchinchi qatlam - LOG va Audit jurnal

Xavfsizlikni ta’minlashning yana bir muhim jihati barcha harakatlarning uzluksiz loglanishi hisoblanadi. Portal orqali amalga oshirilgan har bir jarayon LOG hujjatida qayd etiladi, shu bilan birga Autentifikatsiya blokidan o‘tgan harakatlar Audit jurnal orqali VAAT tizimida alohida ro‘yxatga olinadi. Bu ikki mexanizm - LOG va Audit jurnal - tizimda sodir bo‘lgan har qanday amalni (kirish, xatolik, so‘rov) keyinchalik tekshirish va zarur bo‘lganda javobgarlikni aniqlash imkonini beruvchi nazorat vositasi hisoblanadi. Bunday mexanizm ISO/IEC 27001:2022 standartining A.12.4 nazorat sohasi (Logging and monitoring) talablariga to‘liq muvofiq keladi.

To‘rtinchi qatlam -Ma’lumotlarni saqlash va boshqarish

Ma’lumotlarning xavfsiz saqlanishi esa Ma’lumotlarni saqlash va boshqarish bloki orqali ta’minlanadi. Bu blok PostgreSQL asosiy ma’lumotlar bazasi va Kesh xotira bilan bog‘liq holda ishlaydi. PostgreSQL- ACID (Atomicity, Consistency, Isolation, Durability) prinsiplariga muvofiq ishlaydigan ochiq kodli relatsion ma’lumotlar bazasi bo‘lib, tizim uchun asosiy saqlash mexanizmini ta’minlaydi. Kesh xotira esa tez-tez murojaat qilinadigan ma’lumotlarga tezkor kirishni ta’minlab, tizimning ishlash tezligini oshiradi. Natijada tizim ichida aylanayotgan ma’lumotlar tartiblangan, nazorat qilinadigan muhitda saqlanadi va tasodifiy yoki ruxsatsiz o‘zgartirishlardan himoyalangan holda boshqariladi.

Arxitekturaning yaxlit ishlashi

Tahlil natijalari shuni ko‘rsatdiki, taklif etilgan to‘rt qatlamli xavfsizlik arxitekturasining har bir komponenti alohida ishlaganda ma’lum bir vazifani bajaradi, biroq ularning eng katta samarasi qatlamlarning uzviy bog‘langan holda birgalikda ishlashida namoyon bo‘ladi.

Autentifikatsiya bloki foydalanuvchini tasdiqlaydi, Karrali nazorat noto‘g‘ri so‘rovlarni chiqarib tashlaydi, LOG va Audit jurnal barcha harakatlarni qayd etadi, Ma’lumotlarni saqlash va boshqarish bloki esa ma’lumotlarni nazoratli tarzda saqlaydi.

Bu qatlamlarning ketma-ket va bir vaqtning o‘zida ishlashi tizimga faqat tekshiruvdan o‘tgan, qonuniy so‘rovlarning kirishini, sodir bo‘lgan har bir amalning esa qayd etilib borishini ta’minlaydi.

Xulosa

Ushbu tadqiqotda VAAT tizimida axborot xavfsizligini ta’minlashning to‘rt qatlamli arxitekturasi - Autentifikatsiya (OneID) → Karrali nazorat → LOG/Audit jurnal → PostgreSQL/Kesh saqlash -taklif etildi va uning ilmiy-amaliy asoslari ochib berildi. Taklif etilgan model ISO/IEC 27001:2022 xalqaro standarti va O‘z DSt 2590:2012 milliy standarti talablariga muvofiqlashtirilgan bo‘lib, veterinariya sohasidagi elektron xizmatlarni ko‘rsatishda ma’lumotlarning yaxlitligini, maxfiyligini va foydalanish qulayligini bir vaqtning o‘zida ta’minlashga xizmat qiladi.

Tadqiqotning amaliy ahamiyati shundaki, taklif etilgan arxitektura nafaqat VAAT tizimida, balki O‘zbekistondagi boshqa elektron davlat xizmatlarining xavfsizligini ta’minlashda ham universal shablon sifatida qo‘llanilishi mumkin.

Kelajakdagi tadqiqotlar yo‘nalishi sifatida sun’iy intellekt asosidagi anomaliyalarni aniqlash mexanizmlarini mavjud arxitekturaga integratsiyalash va blokcheyn texnologiyasi yordamida audit izining buzilmasligini kuchaytirish masalalari tavsiya etiladi.

FOYDALANILGAN ADABIYOTLAR:

1. O‘zbekiston Respublikasi. "Axborotlashtirish to‘g‘risida"gi Qonun (O‘RQ-560-son, 2003-yil 11-dekabr).

2. O‘z DSt 2590:2012. Axborot texnologiyalari. Davlat axborot tizimlarining o‘zaro hamkorligiga (interoperabellik) qo‘yiladigan asosiy talablar. -Toshkent: O‘zstandart, 2012.- 16 b.

3. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection - Information security management systems- Requirements. -Geneva: ISO, 2022.

4. ISO/IEC 25012:2008. Software engineering - Software product Quality Requirements and Evaluation (SQuaRE)- Data quality model. - Geneva: ISO, 2008.

5. Smith J., Brown T., Wilson A. Information reliability in government systems // IEEE Access. - 2021. - Vol. 9. - P. 12345–12360.

6. Lee K., Park S., Kim J. Multi-stage authentication and data validation models // Computers & Security. -2022.- Vol. 118. - P. 102–120.

7. Brown A. Data integrity and reliability in public sector IT systems // Government Information Quarterly. -2023. - Vol. 40, Iss. 2. - P. 101–115.

8. Shukla R., Patel N. Software reliability modeling using failure intensity approach // Journal of Systems and Software. - 2020. -Vol. 165. -P. 110–125.

9. Sato K., Nakamura Y. Backup and recovery mechanisms in large-scale information systems // IEEE Systems Journal. - 2021. - Vol. 15, No. 3.- P. 4321–4335.

10. Raxmanov Q.S., Rustamova M.Ya. Veterinariya yagona axborot tizimini ishlab chiqish jarayonlari // Open Academia: Journal of Scholarly Research. -2024.- T. 2, № 6. - B. 57–61.