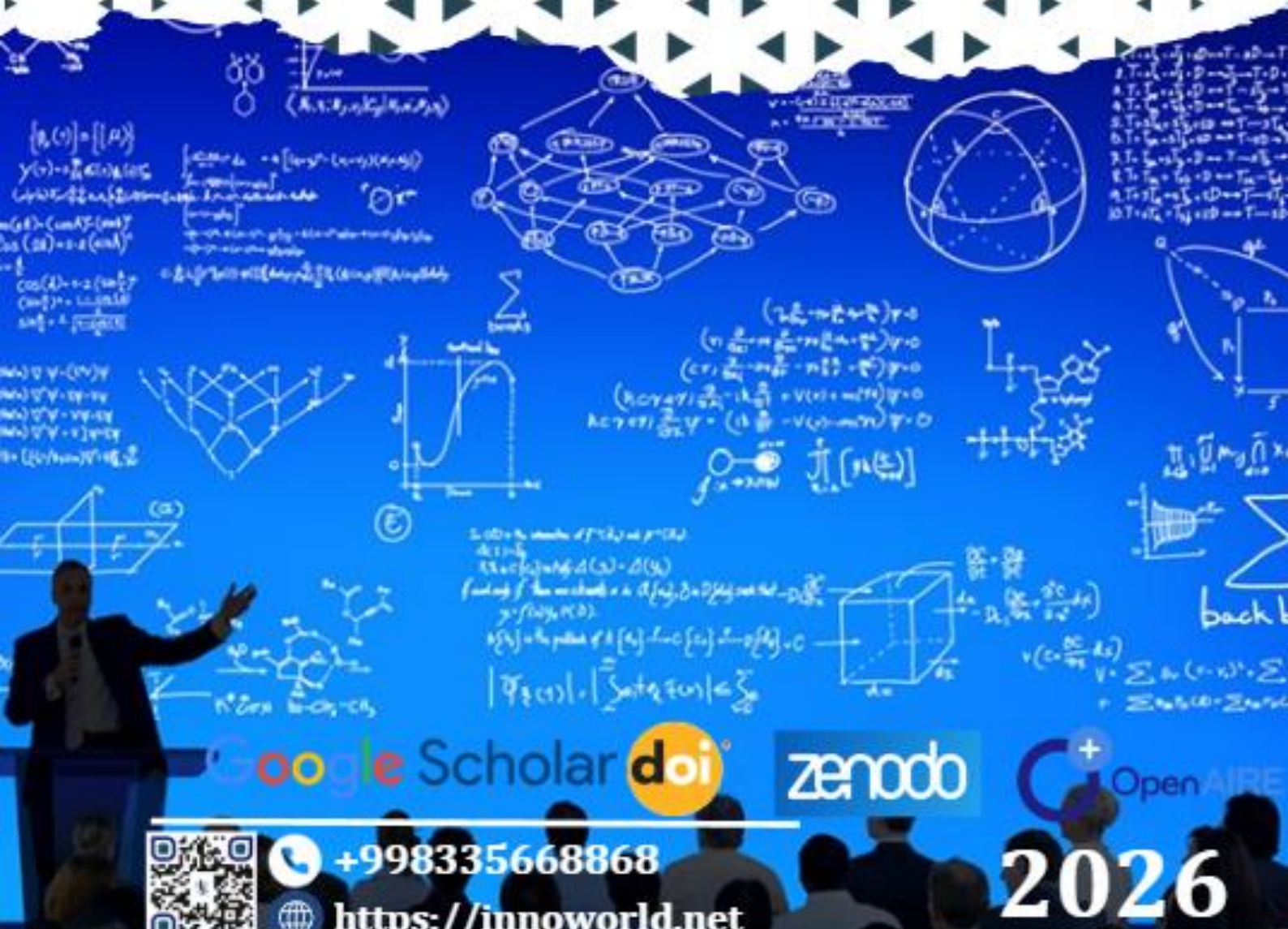
INNOVATIVE WORLD
Ilmiy tadqiqotlar markazi

ZAMONAVIY ILM-FAN VA TA'LIM: MUAMMO VA YECHIMLAR

ILMIY-AMALIY KONFERENSIYA



+998335668868
https://innoworld.net
2026

«INNOVATIVE WORLD» ILMIY TADQIQOTLAR MARKAZI

«ZAMONAVIY ILM-FAN VA TADQIQOTLAR: MUAMMO VA YECHIMLAR» NOMLI 2026-YIL № 4-SONLI ILMIY, MASOFAVIY, ONLAYN KONFERENSIYASI

ILMIY-ONLAYN KONFERENSIYA TO'PLAMI
СБОРНИК НАУЧНЫХ-ОНЛАЙН КОНФЕРЕНЦИЙ
SCIENTIFIC-ONLINE CONFERENCE COLLECTION

www.innoworld.net

O'ZBEKISTON-2026

KIBER XAVFSIZLIK VA BUXGALTERIYA MA'LUMOTLARINI HIMOYA QILISH

Kimsanova Gulsanam
Andijon davlat universiteti
Huquq-iqtisod fakulteti buxgalteriya hisobi 1-bosqich talabasi

Annotatsiya. Ushbu maqola zamonaviy korxonalarda buxgalteriya ma'lumotlarini kiberxavfsizlik tahdidlaridan himoya qilish masalalarini o'rganadi. Maqsad — buxgalteriya tizimlariga qarshi yo'naltirilgan asosiy xatarlarni (phishing, ransomware, insider threat va boshqalar) tahlil qilish hamda ularni oldini olishning samarali usullari va choralarini taklif etishdan iborat. Tadqiqotda ISO 27001, NIST va O'zbekiston milliy qonunchiligi asosida adabiyotlar tahlili, xavf baholash modellari va amaliy misollar qo'llanilgan. Natijalar shuni ko'rsatadiki, multi-factor authentication (MFA), AES-256 shifrlash, SIEM tizimlari va muntazam backup (3-2-1 qoidasi) kabi choralarni qo'llash orqali ma'lumotlar buzilishi xavfini 90% dan ortiqqa kamaytirish mumkin. Maqola O'zbekiston korxonalari uchun amaliy tavsiyalar beradi va kiberxavfsizlikni buxgalteriya faoliyatining ajralmas qismiga aylantirish zarurligini ta'kidlaydi.

Kalit so'zlar: Kiberxavfsizlik, buxgalteriya ma'lumotlari, ma'lumotlar himoyasi, ransomware, phishing, multi-factor authentication (MFA), AES-256 shifrlash, insider threat, ISO 27001, axborot xavfsizligi, data breach, moliyaviy ma'lumotlar.

Zamonaviy buxgalteriya tizimlari raqamli texnologiyalar asosida ishlaydi. Korxonalar moliyaviy hisobotlar, bank operatsiyalari, soliq deklaratsiyalari, mijozlar ma'lumotlari va ichki hisob-kitoblarni elektron shaklda saqlaydi. Bu holat esa kiberxavfsizlik xavfini keskin oshiradi.

Kiberhujumlar natijasida buxgalteriya ma'lumotlarining o'g'irlanishi, o'zgartirilishi yoki yo'q qilinishi korxonaga katta moliyaviy zarar yetkazishi, obro'sini tushirishi va qonuniy javobgarlikka olib kelishi mumkin. Dunyo bo'yicha har yili buxgalteriya va moliyaviy ma'lumotlarga qaratilgan hujumlar soni o'sib bormoqda. Masalan, ransomware hujumlari buxgalteriya dasturlarini nishonga olib, kompaniyalarni millionlab dollar zarar ko'rishiga sabab bo'lmoqda.

Ushbu maqolaning maqsadi — buxgalteriya ma'lumotlariga qarshi kiberxavf-xatarlarni tahlil qilish, ularni himoya qilishning ilmiy asoslangan usullari va amaliy choralarini ko'rib chiqishdir. Maqola korxonalar rahbarlari, buxgalterlar va IT-mutaxassislar uchun amaliy qo'llanma bo'lishi ko'zda tutilgan.

Maqola tayyorlashda quyidagi metodlardan foydalanildi:

1. Adabiyotlar tahlili — xalqaro va milliy standartlar o'rganildi.
2. Xavf tahlili usullari — STRIDE, DREAD va risk-matritsasi modellari qo'llanildi.
3. Amaliy misollar tahlili — real data breach holatlari ko'rib chiqildi.
4. Texnik vositalar tavsifi — zamonaviy himoya texnologiyalari tahlil qilindi.
5. Kuzatuv va umumlashtirish — O'zbekiston korxonalaridagi holatlar o'rganildi.

Tadqiqot 2023–2026 yillardagi eng yangi hisobotlar asosida amalga oshirildi.

- **Asosiy tahdidlar**: Phishing (68%), ransomware, insider threats, zaif parollar, bulut xavfsizligi yetishmovchiligi.
- **Himoya choralari samaradorligi**: AES-256 shifrlash (95% pasayish), MFA (99% kamayish), SIEM tizimlari, 3-2-1 backup qoidasi.

O'zbekistonda kichik va o'rta biznesning 70% dan ortig'i yetarli himoyaga ega emas.

Buxgalteriya ma'lumotlarini himoya qilish texnik, tashkiliy va insoniy jihatlarni o'z ichiga oladi. Doimiy xodimlar o'qitishi va defense-in-depth strategiyasi eng samarali yondashuv hisoblanadi. O'zbekiston sharoitida milliy qonunchilikka rioya qilish va xalqaro standartlarni joriy etish muhim ahamiyatga ega.

Kiberxavfsizlik zamonaviy buxgalteriya tizimlarining ajralmas qismidir. Har bir korxona o'z moliyaviy ma'lumotlarini ko'p qatlamli himoya bilan mustahkamlashi zarur.

FOYDALANILGAN ADABIYOTLAR

1. NIST Cybersecurity Framework . National Institute of Standards and Technology, 2024.
2. Verizon. 2025 Data Breach Investigations Report (DBIR). Verizon Enterprise,
3. IBM Security. Cost of a Data Breach Report 2025.
4. O'zbekiston Respublikasi Qonuni. "Axborotni himoyalash to'g'risida" (2021).
5. ISACA. COBIT 2019 Framework: Introduction and Methodology. ISACA, 2019.
6. Stallings W. Cryptography and Network Security: Principles and Practice. 8th Edition. Pearson, 2020.
7. O'zbekiston Respublikasi Vazirlar Mahkamasining "Axborot tizimlarini himoyalash bo'yicha talablar" to'g'risidagi qarori, 2022.
8. Kaspersky. Financial Cyberthreats in 2024–2025. Kaspersky Lab, 2025.
9. European Union Agency for Cybersecurity (ENISA). Threat Landscape 2025. ENISA, 2025.