JURNALLAR (LOG) VA MONITORING: KORXONADA SHUBHALI HARAKATLARNI ANIQLASH VA ICHKI FIRIBGARLIKNING OLDINI OLISH

Samarqand iqtisodiyot va servis instituti

"XALQARO IQTISODIY MUNOSABATLAR" fakulteti

.Iqtisodiy xavfsizlik yo‘nalishi

IKX-123 4-KURS

Raxmatova Yasmina Dilshodjon qizi

+998949791888

or284887@gmail.com

Samarqand iqtisodiyot va servis instituti

Axborot texnologiyalari kafedrasi asistenti

Rustamov Sherzod Norxudjayevich

Annotatsiya: Maqolada korxona axborot tizimlarida hodisalar jurnallarini (log) yuritish va ularni monitoring qilishning ichki firibgarlikni aniqlash hamda oldini olishdagi o‘rni ilmiy-huquqiy jihatdan tahlil qilinadi. Tadqiqotning maqsadi — O‘zbekiston Respublikasi normativ-huquqiy bazasi va xalqaro tajriba asosida jurnallashtirish va monitoring tizimini tashkil etishning samarali, qonuniy va xodim huquqlariga mutanosib modelini ilmiy va amaliy jihatdan asoslashdan iborat. Mavzuning dolzarbligi so‘nggi yillarda raqamli xizmatlarning kengayishi, moliyaviy va axborot jarayonlarining avtomatlashtirilishi hamda ichki shaxslar tomonidan sodir etiladigan huquqbuzarliklar zararining yuqoriligi bilan belgilanadi. Tadqiqotda qiyosiy-huquqiy tahlil, tizimli yondashuv, ilmiy adabiyotlar va xalqaro standartlar (NIST SP 800-92, ISO/IEC 27001) mazmunini taqqoslash hamda miqdoriy illyustrativ hisob-kitob usullaridan foydalanildi. Olingan natijalar shuni ko‘rsatdiki, jurnallar faqat texnik yozuv emas, balki “firibgarlik uchburchagi”dagi imkoniyat omilini cheklovchi nazorat vositasidir; ularning ishonchliligi markazlashtirish, yaxlitlikni ta’minlash va vazifalarni taqsimlash bilan belgilanadi;

anomaliyalarni aniqlash usullari esa yolg‘on signallar muammosini inobatga olgan holda qo‘llanishi lozim. Maqolada normativ-huquqiy, tashkiliy va texnik takliflar hamda korxonalar, jumladan, davlat tashkilotlari uchun amaliy tavsiyalar shakllantirildi.

Kalit so‘zlar: jurnallar (log), monitoring, ichki firibgarlik, shubhali harakatlar, anomaliyalarni aniqlash, ichki nazorat, kiberxavfsizlik, audit izi, firibgarlik uchburchagi, shaxsga doir ma’lumotlar.

Abstract: The article provides a scientific and legal analysis of the role of event logging and monitoring in corporate information systems in detecting and preventing internal fraud. The aim of the study is to substantiate an effective, lawful, and proportionate model of logging and monitoring based on the regulatory framework of the Republic of Uzbekistan and international experience. The relevance of the topic is determined by the expansion of digital services, the automation of financial and information processes, and the high losses caused by violations committed by insiders. Comparative legal analysis, a systemic approach, a comparison of the scientific literature and international standards (NIST SP 800-92, ISO/IEC 27001), and illustrative quantitative calculations were used as research methods. The results demonstrate that logs are not merely technical records but a control instrument that limits the opportunity element of the “fraud triangle”; that their reliability depends on centralization, integrity protection, and segregation of duties; and that anomaly detection methods should be applied with due regard to the false-positive problem. Normative-legal, organizational, and technical proposals, as well as practical recommendations for enterprises, are formulated in the article.

Keywords: logs, monitoring, internal fraud, suspicious activity, anomaly detection, internal control, cybersecurity, audit trail, fraud triangle, personal data.

KIRISH

Raqamli transformatsiya sharoitida korxonalarning moliyaviy, kadrlar va ishlab chiqarish jarayonlari axborot tizimlarida amalga oshirilmoqda. Bu jarayonning teskari tomoni shundaki, tizimlarga qonuniy kirish huquqiga ega xodimlar — ya’ni ichki shaxslar

— tashqi hujumchiga nisbatan ancha katta imkoniyatga ega bo‘ladi. Ichki firibgarlik (occupational fraud) deganda xodimning o‘z lavozimidan tashkilot resurslari yoki aktivlarini suiiste’mol qilish orqali shaxsiy manfaat ko‘rish maqsadida foydalanishi tushuniladi. Sertifikatlangan firibgarlik tekshiruvchilari assotsiatsiyasi (ACFE) 2024-yilgi hisobotida tashkilotlar yillik daromadining taxminan 5 foizini bunday firibgarlik tufayli yo‘qotishi, bir holat bo‘yicha mediana zarar 145 ming AQSh dollarini, firibgarlikning aniqlanishiga qadar o‘tgan mediana muddat esa taxminan 12 oyni tashkil etishini qayd etgan.[1] Demak, muammo faqat zararning miqdorida emas, balki uning uzoq vaqt sezilmay qolishidadir; aynan shu bo‘shliqni jurnallar va monitoring yopishi mumkin.

Mavzuning huquqiy dolzarbligi konstitutsiyaviy normalardan boshlanadi. O‘zbekiston Respublikasi Konstitutsiyasining 2023-yilgi yangi tahririda mulk daxlsizligi bilan bir qatorda shaxsiy hayot daxlsizligi va shaxsga doir ma’lumotlarni himoya qilish huquqi ham kafolatlangan.[2] Bu ikki konstitutsiyaviy qadriyat o‘rtasidagi muvozanat jurnallashtirish masalasining mohiyatini belgilaydi: korxona o‘z mulki va ma’lumotlarini himoya qilish uchun xodimlar harakatini qayd etishga haqli, biroq bunday nazorat qonuniy, aniq maqsadga yo‘naltirilgan va mutanosib bo‘lishi shart. Jurnal yozuvlarida xodimning identifikatori, kirish vaqti va bajargan amallari aks etgani sababli, ular o‘zi shaxsga doir ma’lumot hisoblanadi va 2019-yil 2-iyuldagi O‘RQ-547-son “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonun talablariga, jumladan, maqsadga muvofiqlik, saqlash va himoya qilish tamoyillariga bo‘ysunadi.[3] Xodimlar bilan munosabatlar esa Mehnat kodeksi normalari bilan tartibga solinadi.[4]

[1]Association of Certified Fraud Examiners. Occupational Fraud 2024: A Report to the Nations. — Austin: ACFE, 2024. URL: https://www.acfe.com/report-to-the-nations

[2]O‘zbekiston Respublikasi Konstitutsiyasi (2023-yil 30-aprelda umumxalq referendumida qabul qilingan yangi tahriri), 31-modda // Milliy qonunchilik ma’lumotlari bazasi (Lex.uz). URL: https://lex.uz

[3]O‘zbekiston Respublikasining 2019-yil 2-iyuldagi O‘RQ-547-son “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni // Lex.uz. URL: https://lex.uz

[4]O‘zbekiston Respublikasi Mehnat kodeksi (2022-yil 28-oktabrdagi O‘RQ-798-son) // Lex.uz. URL: https://lex.uz

Sohaning qonunchilik asosini yana bir qator hujjatlar tashkil etadi. 2022-yil 15-apreldagi O‘RQ-764-son “Kiberxavfsizlik to‘g‘risida”gi Qonun kiberxavfsizlik sohasidagi munosabatlarni, subyektlarning vakolat va majburiyatlarini hamda muhim axborot infratuzilmasini himoya qilish asoslarini belgilab, kiberhodisalarni aniqlash va ularga javob berishni tizimli faoliyat sifatida mustahkamlagan.[5] 2017-yil 3-yanvardagi O‘RQ-419-son “Korrupsiyaga qarshi kurashish to‘g‘risida”gi Qonun korrupsiyaning oldini olishga qaratilgan choralarni belgilaydi,[6] 2021-yil 13-apreldagi O‘RQ-686-son “Buxgalteriya hisobi to‘g‘risida”gi Qonun esa xo‘jalik yurituvchi subyektlarda hisob ma’lumotlarining ishonchliligi va ichki nazorat tizimi masalalarini tartibga soladi.[7] Jurnallar va monitoring aynan ushbu normalarning amaliy ijrosini ta’minlovchi texnik vosita bo‘lib xizmat qiladi: ular hisob ma’lumotlarini kim va qachon o‘zgartirganini isbotlash imkonini beradi.

Strategik darajada 2020-yil 5-oktabrdagi PF-6079-son Farmon bilan tasdiqlangan “Raqamli O‘zbekiston — 2030” strategiyasi davlat va tijorat sektorida jarayonlarni raqamlashtirishni jadallashtirdi,[8] bu esa nazorat mexanizmlarini ham raqamli muhitga ko‘chirish zaruratini keltirib chiqardi. Jinoyat-huquqiy jihatdan Jinoyat kodeksining mulkni o‘zlashtirish yoki rastrata qilish (167-modda), firibgarlik (168-modda) hamda axborot texnologiyalari sohasidagi jinoyatlar (XX¹ bob) uchun javobgarlikni nazarda tutuvchi normalari ichki firibgarlik holatlarini baholashda asos bo‘ladi,[9] bunda jurnal yozuvlari dalil sifatida muhim ahamiyat kasb etadi. Biroq normativ bazada jurnallarni

[5]O‘zbekiston Respublikasining 2022-yil 15-apreldagi O‘RQ-764-son “Kiberxavfsizlik to‘g‘risida”gi Qonuni // Lex.uz. URL: https://lex.uz

[6]O‘zbekiston Respublikasining 2017-yil 3-yanvardagi O‘RQ-419-son “Korrupsiyaga qarshi kurashish to‘g‘risida”gi Qonuni // Lex.uz. URL: https://lex.uz

[7]O‘zbekiston Respublikasining 2021-yil 13-apreldagi O‘RQ-686-son “Buxgalteriya hisobi to‘g‘risida”gi Qonuni // Lex.uz. URL: https://lex.uz

[8]O‘zbekiston Respublikasi Prezidentining 2020-yil 5-oktabrdagi PF-6079-son Farmoni bilan tasdiqlangan “Raqamli O‘zbekiston — 2030” strategiyasi // Lex.uz. URL: https://lex.uz

[9]O‘zbekiston Respublikasi Jinoyat kodeksi (1994-yil 22-sentabrdagi 2012-XII-son Qonun bilan tasdiqlangan), 167-, 168-moddalar va XX¹ bob // Lex.uz. URL: https://lex.uz

yuritishning aniq texnik mezonlari (nimalar yozilishi, qancha saqlanishi, yaxlitligi qanday ta’minlanishi) yetarlicha batafsil belgilanmagan. Mazkur tadqiqotning maqsadi shu bo‘shliqni xalqaro standartlar va ilmiy tadqiqotlar asosida to‘ldiruvchi model va takliflarni ishlab chiqishdan iborat; tadqiqotda qiyosiy-huquqiy tahlil, standartlarni taqqoslash va miqdoriy illyustrativ hisob usullari qo‘llanildi.

Ichki firibgarlikning ilmiy tushuntirishi D. Kressining 1953-yildagi “firibgarlik uchburchagi” nazariyasiga tayanadi: shaxs firibgarlikka bosim (moliyaviy muammo), imkoniyat (nazoratning zaifligi) va o‘zini oqlash (rationalizatsiya) uyg‘unlashganda boradi.[10] D. Vulf va D. Hermanson bu modelni “firibgarlik olmosi”gacha kengaytirib, to‘rtinchi omil sifatida shaxsning qobiliyatini (lavozimi, tizimni bilishi) qo‘shgan.[11] Bu omillar ichida tashkilot ta’sir qila oladigani birinchi navbatda imkoniyatdir. Jurnallar va monitoring imkoniyatni ikki yo‘l bilan cheklaydi: ular firibgarlikni aniqlashni tezlashtiradi va, ayniqsa muhimi, “aniqlanish ehtimoli yuqori” degan sub’ektiv idrokni shakllantirib, to‘xtatuvchi omil vazifasini bajaradi. ACFE ma’lumotlariga ko‘ra, holatlarning eng katta qismi (taxminan 43 foizi) xabarlar (tip) orqali aniqlangan bo‘lsa-da, proaktiv ma’lumotlar monitoringi qo‘llangan tashkilotlarda zarar kichikroq va aniqlash muddati qisqaroq bo‘lgan; shu sababli ishonch liniyasi va texnik monitoring bir-birini to‘ldiruvchi vositalar sifatida qaralishi kerak.

Ichki tahdidlar bo‘yicha CERT (Karnegi-Mellon universiteti) tadqiqotchilari yuzlab real holatlarni tahlil qilib, ichki shaxslar tomonidan sodir etilgan firibgarlik, ma’lumot o‘g‘irlash va sabotaj holatlari ko‘pincha aniqlanishi mumkin bo‘lgan texnik va xulq-atvoriy belgilar bilan kechishini, ya’ni “iz” qoldirishini ko‘rsatgan.[12] Amaliy jihatdan bu shuni anglatadiki, tizim hodisalarni qayd etmasa, tergov va ichki audit dalilsiz qoladi.

[10]Cressey D.R. Other People’s Money: A Study in the Social Psychology of Embezzlement. — Glencoe, IL: Free Press, 1953.

[11]Wolfe D.T., Hermanson D.R. The Fraud Diamond: Considering the Four Elements of Fraud // The CPA Journal. — 2004. — Vol. 74, No. 12. — P. 38–42.

[12]Cappelli D.M., Moore A.P., Trzeciak R.F. The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes. — Upper Saddle River: Addison-Wesley, 2012.

Jurnallarni boshqarish bo‘yicha NIST SP 800-92 qo‘llanmasi jurnal manbalarini aniqlash, ularni markazlashtirilgan saqlash, ma’lumotlarni normallashtirish, saqlash muddatlarini belgilash va muntazam tahlil qilishni tavsiya etadi.[13] ISO/IEC 27001:2022 standartining 8.15 va 8.16-nazoratlari esa tashkilotdan faoliyat jurnallarini yuritish, ularni himoyalash va tarmoq hamda tizimlardagi g‘ayritabiiy xulq-atvorni monitoring qilishni talab qiladi.[14] Eng kamida har bir muhim hodisa “kim, nima, qachon, qayerdan va qanday natija bilan” savollariga javob beradigan tarzda qayd etilishi, barcha tizimlarda vaqt sinxronlashtirilishi lozim, aks holda turli tizimlar yozuvlarini bog‘lab bo‘lmaydi.

Jurnalning dalillik qiymati uning yaxlitligiga bog‘liq: agar firibgarlikni sodir etgan shaxs, ayniqsa imtiyozli foydalanuvchi, o‘z izlarini o‘chira olsa, monitoring ma’nosini yo‘qotadi. B. Shnayer va J. Kelsi buzilgan tizimda ham oldingi yozuvlarni yashirin o‘zgartirish imkonini bermaydigan kriptografik himoyalangan audit jurnallari sxemasini taklif etgan.[15] Amaliy darajada bu jurnallarni alohida, faqat qo‘shish (append-only) rejimida ishlaydigan markaziy omborga uzatish, administratorlarning jurnalga o‘zgartirish kiritish huquqini cheklash va yozuvlar xeshlarini mustaqil kontur orqali tasdiqlashni anglatadi. Bundan tashqari, nazorat vazifalarni taqsimlash tamoyiliga tayanishi kerak: D. Klark va D. Uilson tijorat tizimlarida firibgarlikning oldini olishning asosiy mexanizmlaridan biri sifatida ma’lumotlar yaxlitligini ta’minlovchi “yaxshi shakllangan tranzaksiyalar” va vazifalarni ajratishni asoslagan.[16] Misol uchun, yetkazib beruvchining bank rekvizitlarini o‘zgartirgan xodim to‘lovni tasdiqlay olmasligi kerak; jurnallar esa bu qoida buzilgan hollarni aniqlaydi.

[13]Kent K., Souppaya M. Guide to Computer Security Log Management. NIST Special Publication 800-92. — Gaithersburg: NIST, 2006.

[14]ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Annex A, controls 8.15 (Logging) and 8.16 (Monitoring activities). — Geneva: ISO/IEC, 2022.

[15]Schneier B., Kelsey J. Secure audit logs to support computer forensics // ACM Transactions on Information and System Security. — 1999. — Vol. 2, No. 2. — P. 159–176.

[16]Clark D.D., Wilson D.R. A Comparison of Commercial and Military Computer Security Policies // Proceedings of the 1987 IEEE Symposium on Security and Privacy. — IEEE, 1987. — P. 184–194.

Monitoringda ikki yondashuv uyg‘unlashtiriladi: qoidalarga asoslangan va statistik. Qoidalarga asoslangan usul ma’lum xavf belgilarini kuzatadi: ish vaqtidan tashqari kirishlar, ruxsatsiz imtiyozlarni oshirish, ma’lumotlarni ommaviy eksport qilish, hech ishlatilmagan (“uxlab yotgan”) hisoblarning faollashuvi, tasdiqlash limitidan bir oz past summadagi takroriy tranzaksiyalar, yetkazib beruvchi rekvizitlarining o‘zgartirilishi. Statistik usullardan biri raqamlarning birinchi raqam bo‘yicha taqsimotini tahlil qiluvchi Benford qonunidir: tabiiy hosil bo‘lgan moliyaviy ma’lumotlarda birinchi raqam 1 bo‘lish ehtimoli $\log_{10}(2) \approx 30{,}1$ foiz, 9 bo‘lish ehtimoli esa $\log_{10}(10/9) \approx 4{,}6$ foiz; sun’iy kiritilgan yoki limitga moslashtirilgan summalar bu taqsimotdan sezilarli chetlanadi va qo‘shimcha tekshiruvga undaydi.[17] V. Chandola va hamkasblarining umumlashtiruvchi tadqiqoti anomaliyalarni aniqlash usullarini (statistik, klasterlashga, yaqinlikka asoslangan va boshqalar) tasniflab, usul tanlovi ma’lumot turi va “normal xulq-atvor” ta’rifiga bog‘liqligini ko‘rsatgan.[18] A. Tuor va hamkasblari esa ichki tahdidni aniqlash uchun tizim jurnallaridagi odatiy xulq-atvorni nazoratsiz o‘rganuvchi chuqur neyron tarmoqlardan foydalanish mumkinligini ko‘rsatgan.[19]

Biroq yuqori texnologiyali vositalarning cheklovi bor: yolg‘on signallar muammosi. Buni oddiy hisob-kitob bilan ko‘rsatish mumkin (mualliflik illyustrativ hisobi). Faraz qilaylik, 10 000 xodimli tashkilotda 10 nafar xodim haqiqatan g‘arazli harakat qilmoqda, detektor ularning 90 foizini topadi (9 ta to‘g‘ri signal), lekin halol xodimlarning 1 foizini ham noto‘g‘ri belgilaydi (taxminan 100 ta yolg‘on signal). Bunda signallarning faqat taxminan 8 foizi haqiqiy bo‘ladi: $9 / (9 + 100) \approx 8{,}3$ foiz. Bu hodisa nodir hodisalar uchun xos “bazaviy darajani e’tiborsiz qoldirish” xatosiga bog‘liq. Demak, monitoring natijasi ayblov emas, balki tekshiruv uchun signal sifatida talqin qilinishi, signallar xavf darajasi

[17]Nigrini M.J. Benford’s Law: Applications for Forensic Accounting, Auditing, and Fraud Detection. — Hoboken: Wiley, 2012.

[18]Chandola V., Banerjee A., Kumar V. Anomaly detection: A survey // ACM Computing Surveys. — 2009. — Vol. 41, No. 3. — Article 15.

[19]Tuor A., Kaplan S., Hutchinson B., Nichols N., Robinson S. Deep Learning for Unsupervised Insider Threat Detection in Structured Cybersecurity Data Streams // Workshops at the Thirty-First AAAI Conference on Artificial Intelligence. — AAAI Press, 2017.

bo‘yicha ustuvorlashtirilishi va har bir holat inson tomonidan ko‘rib chiqilishi lozim; aks holda halol xodimlarga nisbatan asossiz shubha va mehnat nizolari yuzaga keladi.

Monitoring vaqt bo‘yicha ikki rejimda tashkil etilishi maqsadga muvofiq. Real vaqt rejimida eng xavfli hodisalar (masalan, imtiyozli hisobning kutilmagan yaratilishi yoki yirik to‘lovning limitdan oshishi) bo‘yicha ogohlantirish yuboriladi; retrospektiv rejimda esa jurnallar muntazam (haftalik, oylik) tahlil qilinib, uzoq muddatli tendensiyalar, masalan, bir xodimning bir yetkazib beruvchi bilan takroriy operatsiyalari aniqlanadi. Ichki firibgarlik ko‘pincha bir martalik hodisa emas, balki uzoq davom etuvchi jarayon bo‘lgani uchun saqlash muddati (kamida bir yillik retrospektiv tahlilni ta’minlaydigan darajada) va arxivlash tartibi oldindan rejalashtirilishi lozim. Monitoring natijalari esa rahbariyat va ichki audit xizmatiga muntazam hisobot sifatida taqdim etilib, nazorat tizimining o‘zini takomillashtirish uchun ishlatilishi kerak.

Monitoring huquqiy-etik chegaralarga rioya qilishi kerak. Yuqorida ko‘rsatilgan konstitutsiyaviy va “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonun talablaridan kelib chiqib, korxona jurnallashtirish maqsadi, yig‘iladigan ma’lumotlar turi, saqlash muddati va foydalanish huquqiga ega shaxslar doirasini ichki hujjatda (axborot xavfsizligi siyosati, mehnat qoidalari) belgilashi va xodimlarni bu haqda oldindan xabardor qilishi lozim. Jurnallarga kirish huquqi minimal doiradagi mas’ul shaxslar bilan cheklanishi, jurnalning o‘zi ham himoya qilinishi kerak. Nazorat usullari xavfga mutanosib bo‘lishi — masalan, kontent emas, metama’lumotlarni tahlil qilish — ham huquqiy, ham axloqiy jihatdan ma’qul. Anomaliya aniqlangan taqdirda hodisaga javob berish tartibi (ichki tekshiruv, dalillarni saqlash zanjiri, huquqiy xizmat va zarur hollarda huquqni muhofaza qilish organlarini jalb qilish) oldindan belgilanishi kerak, chunki noto‘g‘ri to‘plangan dalil keyinchalik huquqiy ahamiyatini yo‘qotadi.

XULOSA

Tadqiqot natijalariga ko‘ra, jurnallar va monitoring ichki firibgarlikka qarshi kurashning texnik tayanchi bo‘lib, “firibgarlik uchburchagi”dagi imkoniyat omilini

cheklaydi hamda to‘xtatuvchi ta’sir ko‘rsatadi. Jurnallarning samaradorligi ularning to‘liqligi, markazlashtirilganligi, vaqt bo‘yicha sinxronligi va yaxlitligining himoyalanganligiga, shuningdek, vazifalarni taqsimlash bilan uyg‘unligiga bog‘liq. Anomaliyalarni aniqlash usullari yolg‘on signallar muammosini inobatga olgan holda, qoidalarga asoslangan va statistik tahlilning birgalikdagi qo‘llanishini talab qiladi. Huquqiy jihatdan monitoring Konstitutsiya va shaxsga doir ma’lumotlar to‘g‘risidagi qonunchilik doirasida, maqsadga muvofiq va mutanosib tarzda amalga oshirilishi shart.

Mualliflik takliflari: 1) muhim axborot tizimlari va moliyaviy jarayonlarda jurnallashtirishning minimal talablarini (qayd etiladigan hodisalar, saqlash muddati, yaxlitlikni ta’minlash) idoraviy yoki milliy uslubiy tavsiya sifatida belgilash va ularni NIST SP 800-92 hamda ISO/IEC 27001 bilan uyg‘unlashtirish; 2) korxonalarda jurnallashtirish va monitoring tartibini ichki hujjatda mustahkamlab, xodimlarni xabardor qilish; 3) jurnallarni alohida, faqat qo‘shish rejimidagi omborga uzatish va imtiyozli foydalanuvchilar faoliyatini alohida nazorat qilish; 4) yuqori xavfli jarayonlarda (to‘lov, yetkazib beruvchi rekvizitlari) vazifalarni ajratish va ikki bosqichli tasdiqlashni joriy etish; 5) texnik monitoringni ishonch liniyasi va xodimlarni o‘qitish bilan uyg‘unlashtirish; 6) mahalliy amaliyotda ichki firibgarlik holatlari bo‘yicha umumlashtirilgan statistik ma’lumotlarni yig‘ish va keyingi ilmiy tadqiqotlar uchun empirik baza yaratish.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

[1] Association of Certified Fraud Examiners. Occupational Fraud 2024: A Report to the Nations. — Austin: ACFE, 2024. URL: https://www.acfe.com/report-to-the-nations

[2] O‘zbekiston Respublikasi Konstitutsiyasi (2023-yil 30-aprelda umumxalq referendumida qabul qilingan yangi tahriri), 31-modda // Milliy qonunchilik ma’lumotlari bazasi (Lex.uz). URL: https://lex.uz

[3] O‘zbekiston Respublikasining 2019-yil 2-iyuldagi O‘RQ-547-son “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni // Lex.uz. URL: https://lex.uz

[4] O‘zbekiston Respublikasi Mehnat kodeksi (2022-yil 28-oktabrdagi O‘RQ-798-son) // Lex.uz. URL: https://lex.uz

[5] O‘zbekiston Respublikasining 2022-yil 15-apreldagi O‘RQ-764-son “Kiberxavfsizlik to‘g‘risida”gi Qonuni // Lex.uz. URL: https://lex.uz

[6] O‘zbekiston Respublikasining 2017-yil 3-yanvardagi O‘RQ-419-son “Korrupsiyaga qarshi kurashish to‘g‘risida”gi Qonuni // Lex.uz. URL: https://lex.uz

[7] O‘zbekiston Respublikasining 2021-yil 13-apreldagi O‘RQ-686-son “Buxgalteriya hisobi to‘g‘risida”gi Qonuni // Lex.uz. URL: https://lex.uz

[8] O‘zbekiston Respublikasi Prezidentining 2020-yil 5-oktabrdagi PF-6079-son Farmoni bilan tasdiqlangan “Raqamli O‘zbekiston — 2030” strategiyasi // Lex.uz. URL: https://lex.uz

[9] O‘zbekiston Respublikasi Jinoyat kodeksi (1994-yil 22-sentabrdagi 2012-XII-son Qonun bilan tasdiqlangan), 167-, 168-moddalar va XX¹ bob // Lex.uz. URL: https://lex.uz

[10] Cressey D.R. Other People’s Money: A Study in the Social Psychology of Embezzlement. — Glencoe, IL: Free Press, 1953.

[11] Wolfe D.T., Hermanson D.R. The Fraud Diamond: Considering the Four Elements of Fraud // The CPA Journal. — 2004. — Vol. 74, No. 12. — P. 38–42.

[12] Cappelli D.M., Moore A.P., Trzeciak R.F. The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes. — Upper Saddle River: Addison-Wesley, 2012.

[13] Kent K., Souppaya M. Guide to Computer Security Log Management. NIST Special Publication 800-92. — Gaithersburg: NIST, 2006.

[14] ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Annex A, controls 8.15 (Logging) and 8.16 (Monitoring activities). — Geneva: ISO/IEC, 2022.

[15] Schneier B., Kelsey J. Secure audit logs to support computer forensics // ACM Transactions on Information and System Security. — 1999. — Vol. 2, No. 2. — P. 159–176.

[16] Clark D.D., Wilson D.R. A Comparison of Commercial and Military Computer Security Policies // Proceedings of the 1987 IEEE Symposium on Security and Privacy. — IEEE, 1987. — P. 184–194.

[17] Nigrini M.J. Benford's Law: Applications for Forensic Accounting, Auditing, and Fraud Detection. — Hoboken: Wiley, 2012.

[18] Chandola V., Banerjee A., Kumar V. Anomaly detection: A survey // ACM Computing Surveys. — 2009. — Vol. 41, No. 3. — Article 15.

[19] Tuor A., Kaplan S., Hutchinson B., Nichols N., Robinson S. Deep Learning for Unsupervised Insider Threat Detection in Structured Cybersecurity Data Streams // Workshops at the Thirty-First AAAI Conference on Artificial Intelligence. — AAAI Press, 2017.