# AXBOROT XAVFSIZLIGI SIYOSATINI BAHOLASH: METODLAR, KATEGORIYALAR VA E'TIBORGA OLINADIGAN OMILLAR

**Vasiyev Nodirbek**
O'zbekiston Milliy universiteti

**Annotatsiya:** Ushbu maqolada axborot xavfsizligi siyosatini (AXS) baholash jarayoni, baholashda qo'llaniladigan asosiy metodlar va kategoriyalar, shuningdek, baholash sifatiga ta'sir etuvchi omillar ilmiy tahlil qilingan. Tadqiqot ISO 27001, NIST, COBIT va GOST R standartlari asosida baholash metodologiyasini ko'rib chiqadi hamda risk-yo'naltirilgan yondashuv va KPI ko'rsatkichlarining rolini ochib beradi. Xulosa sifatida baholash jarayonini samarali tashkil etishga oid tavsiyalar taqdim etilgan.

**Kalit so'zlar:** axborot xavfsizligi, xavfsizlik siyosati, risk baholash, audit, ISO 27001, KPI, gap-tahlil, zararlanish ehtimoli, nazorat samaradorligi, PDCA sikli.

**Аннотация.** В данной статье научно проанализированы процесс оценки политики информационной безопасности (ПИБ), основные методы и категории, применяемые при оценке, а также факторы, влияющие на её качество. Исследование рассматривает методологию оценки на основе стандартов ISO 27001, NIST, COBIT и ГОСТ Р, а также раскрывает роль риск-ориентированного подхода и показателей KPI. В заключение представлены рекомендации по эффективной организации процесса оценки.

**Ключевые слова:** информационная безопасность, политика безопасности, оценка рисков, аудит, ISO 27001, KPI, gap-анализ, ожидаемый ущерб, эффективность контроля, цикл PDCA.

**Abstract.** This article presents a scientific analysis of the information security policy (ISP) evaluation process, the key methods and categories used in assessment, and the factors affecting evaluation quality. The study examines assessment methodology based on ISO 27001, NIST, COBIT, and GOST R standards, and reveals the role of the risk-oriented approach and KPI indicators. Recommendations for the effective organization of the evaluation process are provided as conclusions.

**Keywords:** information security, security policy, risk assessment, audit, ISO 27001, KPI, gap analysis, expected loss, control effectiveness, PDCA cycle.

## Kirish

Zamonaviy raqamli iqtisodiyot sharoitida tashkilotlar tobora ortib borayotgan kibertahdidlarga duch kelmoqda. Axborot xavfsizligi siyosati (AXS siyosati) tashkilotning axborot aktivlarini himoya qilishga qaratilgan asosiy boshqaruv hujjati hisoblanadi va uning samaradorligini muntazam baholash strategik ahamiyat kasb etadi [1]. Biroq amaliyotda ko'plab tashkilotlar AXS siyosatini bir martalik hujjat sifatida qabul qilib, uni yangilamaydi yoki uning amaliy ta'sirini tekshirmaydi, bu esa axborot xavfsizligi tizimidagi jiddiy bo'shliqlarning paydo bo'lishiga olib keladi [2]. Xalqaro standartlar, jumladan ISO/IEC 27001 va NIST SP 800-53, AXS siyosatini vaqti-vaqti bilan baholash va qayta ko'rib chiqishni majburiy talab sifatida belgilaydi [3]. Ushbu maqolaning maqsadi AXS siyosatini baholashning ilmiy asoslangan metodologiyasini, baholash kategoriyalarini va amaliyotda e'tiborga olinadigan omillarni tizimli tarzda taqdim etishdir. Tadqiqot metodologik asosi sifatida xalqaro standartlar va ilmiy adabiyotlar tahlili, shuningdek, risk-yo'naltirilgan baholash tamoyillari qo'llanilgan.

## Metodologiya va adabiyotlar tahlili

Tadqiqotda tizimli adabiyotlar tahlili metodi qo'llanilgan bo'lib, ISO/IEC 27001:2022, NIST SP 800-53, COBIT 2019, GOST R ISO/IEC 27001 va ilmiy jurnallardagi maqolalar asosiy manba sifatida tanlab olingan [3, 4, 5]. Axborot xavfsizligi sohasidagi baholash metodologiyasi zamonaviy tadqiqotlarda asosan ikki yondashuv atrofida shakllanganligini ko'rish mumkin: statik baholash (hujjat tahlili) va dinamik baholash (amaliyotda tekshirish) [6]. Von Solms va Van Niekerk [7] AXS siyosatining

samaradorligi uning mazmuni bilan emas, balki tashkilot ichida qay darajada amalga oshirilishi bilan belgilanishini ta'kidlaydi. Disterer [8] esa ISO 27001 talablarini bajarishning amaliy qiyinchiliklarini tahlil qilib, baholash jarayonida rahbariyat ishtiroki hal qiluvchi omil ekanligini isbotlaydi. Mahalliy ilmiy adabiyotlarda, jumladan O'zbekiston axborot xavfsizligi sohasidagi normativ hujjatlarda ham AXS siyosatini baholash zarurligi ko'rsatib o'tilgan [9]. Xalqaro amaliyotda risk-yo'naltirilgan baholash yondashuvi keng tarqalgan bo'lib, u tashkilotga mavjud xavf-xatarlarni aniqlash, o'lchash va ularni AXS siyosatidagi nazorat mexanizmlari bilan taqqoslash imkonini beradi [10]. Shunday qilib, adabiyotlar tahlili shuni ko'rsatadiki, AXS siyosatini baholash bir tomonlama texnik tekshiruv emas, balki tashkiliy, huquqiy va texnik jihatlarni qamrab olgan ko'p qirrali jarayon sifatida ko'rib chiqilishi zarur.

**Natijalar va muhokama**

Adabiyotlar tahlili va xalqaro standartlar asosida AXS siyosatini baholashning asosiy metodlari, kategoriyalari va e'tiborga olinadigan omillar quyidagicha tizimlashtirish mumkin. Baholashning birinchi va asosiy metodi audit hisoblanadi. Ichki audit ISO 27001 talablari, milliy qonunchilik (masalan, O'zbekiston Respublikasining axborot xavfsizligiga oid normativ-huquqiy hujjatlari) va tashkilot ichki tartib-qoidalariga muvofiqlikni muntazam tekshirishni nazarda tutadi. Tashqi audit esa mustaqil ekspert yoki sertifikatlash organi tomonidan o'tkaziladigan baholashni anglatadi va u tashkilotning axborot xavfsizligi tizimiga nisbatan obyektiv baho berish imkonini yaratadi [3]. Audit jarayonida chek-listlar, hujjatlarni tahlil qilish va tekshiruvlar asosiy vosita sifatida qo'llaniladi.

Risk baholash metodi AXS siyosatini baholashning ikkinchi muhim ustunidir. Sifatli tahlil ekspert bahosi asosida tahdidlar ehtimolini past, o'rta yoki yuqori darajada belgilaydi, miqdoriy tahlil esa yillik kutilayotgan zarar (ALE — Annualized Loss Expectancy) ko'rsatkichi orqali moliyaviy ifodalangan xavfni hisoblashga imkon beradi [6]. Risk baholash AXS siyosatining qanchalik dolzarb xavf-xatarlarni qoplashini va qolgan (residual) risk qabul qilinadigan darajada ekanligini aniqlaydi. Kombinatsiyalashgan yondashuv, ya'ni sifatli va miqdoriy metodlarni birga qo'llash, eng ishonchli natijalarni berishi isbotlangan [10].

Monitorinq va intsidentlarni tahlil qilish metodi AXS siyosatining amaliy samaradorligini o'lchashning bevosita yo'lidir. Axborot xavfsizligi intsidentlari sonini kuzatish, javob berish vaqtini tahlil qilish va takrorlanuvchi buzilishlarni aniqlash AXS siyosatidagi bo'shliqlarni ko'rsatib beradi. Ildiz sabab tahlili (Root Cause Analysis) qaysi sohalarda siyosat ishlamayotganini aniqlashtiradi va korreksion chora-tadbirlar uchun asos bo'ladi [2]. Amaliyotda tekshirish metodi penetratsion testlash (pentest), ijtimoiy muhandislik testlari, zaifliklarni skanerlash va simulyatsiya mashqlari (tabletop exercises) AXS siyosatini real sharoitda sinab ko'rish va zaifliklarga oid empirik ma'lumotlar yig'ish imkonini beradi [4].

Ekspert baholash va so'rovnomalar metodi xodimlarda axborot xavfsizligi siyosati haqidagi xabardorlik darajasini aniqlash uchun qo'llaniladi. Hodimlar orasida o'tkaziladigan so'rovnomalar AXS siyosatining tushunilishi va amalda qanchalik bajarilishini ko'rsatadi. Jarayon egalari va yuqori rahbariyat tomonidan mustaqil baholash esa siyosatning biznes maqsadlariga mos kelishini tekshirish uchun zarurdir [1]. KPI va samaradorlik ko'rsatkichlari baholashning miqdoriy qismini tashkil etadi. Jarayon ko'rsatkichlari o'qitishdan o'tgan xodimlar ulushi, nazorat mexanizmlari bilan qoplangan aktivlar foizi siyosatning joriy etilish darajasini o'lchaydi. Natija ko'rsatkichlari insidentlarni aniqlash va ularga javob berish vaqti (MTTD/MTTR), intsidentlar soni dinamikasi siyosatning haqiqiy samaradorligini aks ettiradi. Iqtisodiy ko'rsatkichlar axborot xavfsizligiga yo'naltirilgan investitsiyalarning daromadliligi (ROI) — AXS siyosatining iqtisodiy asoslanganligini ifodalaydi [5].

Baholash kategoriyalari nuqtai nazaridan AXS siyosati bir nechta asosiy mezonlar bo'yicha tekshirilishi zarur. Standartlar va qonunchilikka muvofiqlik ISO 27001 (ayniqsa 5.2, 9-bandlar va A ilovasi), NIST, GOST R, tarmoq talablari va milliy normativlarga muvofiqligi tekshiriladi. Dolzarblik yangi tahdidlar, texnologiyalar, biznes-jarayonlar va qonunchilik o'zgarishlariga moslashuvi baholanadi. To'liqlik va aniqlik barcha aktivlar va jarayonlarni qamrab olishi, tili xodimlar uchun tushunarli ekanligi, ortiqcha texnik jargonsiz ifodalanganligi ko'rib chiqiladi. Amaliy qo'llanuvchanlik siyosatning kundalik faoliyatda haqiqatan qo'llanilishi, "ko'rinish uchun" emas, balki real boshqaruv vositasi sifatida ishlashi baholanadi. Xabardorlik va muvofiqlik siyosatni bilgan va unga rioya qilayotgan xodimlar ulushi tekshiriladi. Xavf-yo'naltirilganlik siyosat risk baholash natijalarini aks ettirishi va dolzarb tahdidlarga

javob berishi ko‘zda tutiladi. Hujjatlashtirilganlik versiya tarixi, o‘zgarishlar jurnali va rahbariyat tomonidan tasdiqlash mavjudligi talab etiladi [3, 5].

Baholash jarayonida e'tiborga olinadigan qo‘shimcha omillar orasida tashkilot hajmi va tarmoq xususiyatlari (kichik biznes uchun soddaroq siyosat talab etiladi), tashkilot madaniyati va axborot xavfsizligi yetuklik darajasi, manfaatdor tomonlar (xodimlar, mijozlar, hamkorlar) tomonidan berilgan fikr-mulohazalar, shuningdek, tashqi o‘zgarishlar birlashuvlar, yangi yetkazib beruvchilar, bulut xizmatlariga o‘tish alohida ahamiyat kasb etadi [7, 8]. Baholash natijasi bo‘yicha topilmalar va bo‘shliqlar aks ettirilgan hisobot tuzilishi, kerak bo‘lsa siyosat yangilanishi va barcha o‘zgarishlar xodimlarga yetkazilishi lozim. Davriy ko‘rib chiqish ISO 27001 bo‘yicha boshqaruv sharhi (Management Review) yiliga kamida bir marta yoki muhim o‘zgarishlar ro‘y berganda o‘tkazilishini ta’minlash zarur [1, 9].

**Xulosa**

AXS siyosatini baholash bir martalik tekshiruv emas, balki doimiy, tizimli va hujjatlashtirilgan jarayon bo‘lishi kerak. Tadqiqot shuni ko‘rsatadiki, eng samarali yondashuv audit, risk baholash, monitorinq va KPI ko‘rsatkichlarini birlashtiradigan kombinatsiyalashgan metodologiyadir. Baholash faqat axborot xavfsizligi bo‘limi ishi bo‘lib qolmasligi, biznes-bo‘linmalar, yuqori rahbariyat va barcha manfaatdor tomonlar ishtirokida amalga oshirilishi lozim. AXS siyosatining o‘zida baholash tartibi, chastotasi, mas'ul shaxslar va mezonlari mustahkamlab qo‘yilsa, bu jarayon samaradorligi yanada oshadi. Kelajakda AXS siyosatini baholashning avtomatlashtirilgan vositalari va sun'iy intellekt asosidagi tahlil usullarini qo‘llash yo‘nalishida tadqiqotlarni davom ettirish maqsadga muvofiq.

**Adabiyotlar ro‘yxati**

1. Whitman M.E., Mattord H.J. Management of Information Security. 6th ed. Cengage Learning, 2021. 560 b.
2. Calder A., Watkins S. IT Governance: An International Guide to Data Security and ISO 27001/ISO 27002. 7th ed. Kogan Page, 2019. 432 b.
3. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva: ISO, 2022.
4. NIST SP 800-53 Rev. 5. Security and Privacy Controls for Information Systems and Organizations. National Institute of Standards and Technology, 2020.
5. COBIT 2019 Framework: Governance and Management Objectives. ISACA, 2018. 192 b.
6. Peltier T.R. Information Security Risk Analysis. 3rd ed. CRC Press, 2010. 360 b.
7. Von Solms R., Van Niekerk J. From information security to cyber security // Computers & Security. 2013. № 38. B. 97–102.
8. Disterer G. ISO/IEC 27000, 27001 and 27002 for information security management // Journal of Information Security. 2013. № 4(2). B. 92–100.
9. O‘zbekiston Respublikasi Prezidentining 2017-yil 29-fevraldagi PF-3245-son Farmoni "Axborot-kommunikatsiya texnologiyalari sohasida loyiha boshqaruvi tizimini yanada takomillashtirish chora-tadbirlari to‘g‘risida". https://lex.uz/docs/-3324016
10. Shedden P., Scheepers R., Smith W., Ahmad A. Incorporating a knowledge perspective into security risk assessments // VINE Journal of Information and Knowledge Management Systems. 2011. № 41(2). B. 152–166.