WORLD FORUM ON ACADEMIC INNOVATION AND DIGITAL LITERACY

SUN'IY INTELLEKT ASOSIDA TASHKILOTLARDA BIZNES UZLUKSIZLIGINI BOSHQARISH VA KIBERXAVFLAR SHAROITIDA TIKLANISH USTUVORLIGINI ANIQLASH MODELI

t.f.n., dotsent Turdimatov Ma'mirjon Mirzaevich
Farg'ona davlat texnika universiteti, O'zbekiston
turdimatovmamir1958@gmail.com
2-kurs magistranti Aliyev Muhammadali G'ulomjon o'g'li
Farg'ona davlat texnika universiteti, O'zbekiston
muhammadalialiyev083@gmail.com

Annotatsiya: *Tashkilotlarda biznes uzluksizligini ta'minlash uchun biznesga ta'sir tahlili, kiberxavf, xizmatlararo bog'liqlik va sun'iy intellektga asoslangan anomaliya indikatorini birlashtiruvchi gibrid model taklif etiladi. Tiklanish ustuvorligi vaznli indeks orqali baholanib, yakuniy ketma-ketlik texnologik bog'liqliklar hamda vaqt va resurs cheklovlari bilan tekshiriladi. Model shartli hisoblash misolida yoritiladi.*

Kalit so'zlar: *biznes uzluksizligi, kiberxavfsizlik, BIA, sun'iy intellekt, tiklanish ustuvorligi, RTO, RPO.*

Kirish

Kiberhodisa tufayli bir nechta xizmat bir vaqtda to'xtaganda, cheklangan resurslar bilan qaysi jarayonni avval tiklashni aniqlash zarur. Bunda xizmatning biznesdagi ahamiyati, uzilish oqibatlari va boshqa tizimlarga bog'liqligi birgalikda baholanishi kerak. Axborot xavfsizligiga tizimli yondashuv [1] hamda insidentlarga javob berishni tashkil etish [2] ushbu masalaning metodologik asosini tashkil qiladi. Tadqiqot maqsadi biznesga ta'sir tahlili (Business Impact Analysis — BIA) va monitoring signallari asosida tiklanish ustuvorligini tushuntiriladigan tarzda belgilash modelini ishlab chiqishdir.

Biznes uzluksizligini boshqarish tizimi (Business Continuity Management System — BCMS) doirasida texnik tiklash rejasi tashkilotning muhim xizmatlari bilan bog‘lanadi. ISO 22301 BCMS talablarini, ISO 22313 esa ularni qo‘llash bo‘yicha yo‘riqnomani belgilaydi [4, 5]. Axborot xavfsizligi va risklarni boshqarish uchun ISO/IEC 27001, ISO/IEC 27005 hamda ISO 31000 metodologik asos bo‘lib xizmat qiladi [7–9].

Oldindan belgilangan ustuvorlik hodisa ko‘lami va shikastlangan aktivlar haqidagi yangi ma’lumotlarga qarab yangilanishi mumkin. NIST CSF 2.0 va insidentlarga javob berish qo‘llanmasi ushbu faoliyatni kiberxavflarni boshqarish bilan bog‘laydi [12, 13]. Taklif etilayotgan modelda BIA, kiberxavf va monitoring signallari birlashtiriladi; yakuniy rejani mas’ul mutaxassis tasdiqlaydi.

Tadqiqot metodlari va konseptual model

Tadqiqotda tizimli tahlil, ekspert baholash, vaznli ko‘p mezonli saralash va shartli ssenariy asosida hisoblash usullari qo‘llanadi. Dastlab jarayonlar, aktivlar, mas’ul bo‘linmalar va texnik bog‘liqliklar ro‘yxatga olinadi. Har bir i-jarayon uchun [0; 1] oralig‘idagi to‘rtta indikator shakllantiriladi: B_i — uzilishning biznes oqibati; K_i — kiberxavf; D_i — boshqa kritik xizmatlarning ushbu jarayonga bog‘liqligi; A_i — monitoringdagi anomaliya indikatori. Birlamchi ustuvorlik quyidagicha hisoblanadi:

$$P_i = 0{,}40B_i + 0{,}25K_i + 0{,}20D_i + 0{,}15A_i.$$

B_i moliyaviy zarar, xizmat to‘xtashi, obro‘ va majburiyatlarga ta’sirni ifodalaydi; K_i aktiv muhimligi va hodisa oqibatlarini hisobga oladi. D_i yo‘naltirilgan bog‘liqlik grafi asosida aniqlanadi. Sun’iy intellektning vazifasi A_i signalini shakllantirishga ko‘maklashishdan iborat; vaznli indeksning o‘zi o‘rgatilgan model emas. Kalibrlanmagan A_i hodisa ehtimoli sifatida talqin qilinmaydi. Koeffitsiyentlar shartli tanlangan bo‘lib, ekspert bahosi va sezgirlik tahlili orqali tekshirilishi lozim.

BIA mezonlari va baholash shkalasi oldindan ta’riflanishi zarur. ISO/TS 22317 tashkilot ehtiyojiga mos hujjatlashtirilgan BIA jarayonini tashkil etish bo‘yicha



yo‘riqnoma beradi [6]. Moliyaviy zarar, uzilish davomiyligi va majburiyatlarga ta’sir bir xil oraliqqa keltiriladi. Ma’lumot yetishmasa, ekspert taxmini va uning asosi qayd etiladi.

Anomaliya indikatori odatdagi faoliyatdan chetlanishni ifodalaydi; uni shakllantirish usullari Chandola va hammualliflar sharhida tizimlashtirilgan [15]. Yuqori A_i tasdiqlangan hujum yoki hodisa ehtimoli degani emas. Signal manbasi va sifati tekshirilishi, model esa kalibrlanishi kerak. Sun’iy intellektdan foydalanish xavflarini boshqarishda AI RMF yondashuvi hisobga olinishi mumkin [14]. Hozirgi ishda o‘rgatilgan algoritm aniqligi baholanmagan.

Tiklashning maqsadli vaqti (Recovery Time Objective — RTO), ma’lumot yo‘qotishining maqbul vaqt oralig‘i (Recovery Point Objective — RPO) va maksimal yo‘l qo‘yiladigan uzilish davri (Maximum Tolerable Period of Disruption — MTPD) indeksdan alohida cheklovlar sifatida qo‘llanadi. Yakuniy tiklanish tartibi bog‘liqlik grafi va mavjud resurslar bilan muvofiqlashtiriladi. BCMS Designer doirasida BIA, tahdidlar reyestri, monitoring, qaror shakllantirish va audit yozuvlari modullarini birlashtirish nazarda tutiladi. Qaror asoslarini hujjatlashtirish audit uchun muhimdir [3].

Yakuniy tartibda xizmatning tayanch komponentlari, parallel tiklash imkoniyati va mavjud resurslar tekshiriladi. RTO bajarilmaydigan holatlar alohida ko‘rsatiladi. Tiklashni rejalashtirish, resurslarni ustuvorlashtirish va ssenariylarni sinash NIST SP 800-34 hamda SP 800-184 qo‘llanmalarida yoritilgan [10, 11]. Ular taklif etilgan indeks koeffitsiyentlarini yoki uning samaradorligini tasdiqlamaydi.

BCMS Designer uchun ma’lumotlarni yig‘ish, indikatorlarni hisoblash, ustuvorlikni shakllantirish, cheklovlarni tekshirish va qarorni tasdiqlash bosqichlari taklif etiladi. Audit yozuvida qiymatlar, koeffitsiyentlar, hisoblash vaqti va mutaxassis o‘zgartirishlari saqlanadi. Yangi ma’lumotlar asosida baho yangilanadi, amaldagi rejani o‘zgartirish esa mas’ul shaxs bilan kelishiladi.

Natijalar va muhokama

Uchta xizmat uchun (B; K; D; A) qiymatlari to‘lov tizimida (0,95; 0,85; 0,90; 0,80), ombor hisobida (0,70; 0,65; 0,80; 0,50), kadrlar xizmatida (0,50; 0,40; 0,30; 0,20) deb olinsa, P indekslari mos ravishda 0,8925; 0,6775 va 0,3900 bo‘ladi. Dastlabki saralashda to‘lov tizimi birinchi o‘ringa chiqadi. Biroq uning ishlashi autentifikatsiya xizmati yoki ma’lumotlar bazasiga bog‘liq bo‘lsa, ushbu komponentlar avval tiklanadi. Demak, indeks ustuvorlikni bildiradi, lekin bajarilish tartibini yakka o‘zi belgilamaydi.

To‘lov tizimi uchun hisoblash 0,40 × 0,95 + 0,25 × 0,85 + 0,20 × 0,90 + 0,15 × 0,80 = 0,8925 ko‘rinishida bajariladi. Ushbu qiymatdagi eng katta hissa biznes oqibatiga tegishli bo‘lib, 0,38 ni tashkil etadi. Kiberxavf hissasi 0,2125, bog‘liqlik hissasi 0,18 va anomaliya hissasi 0,12 ga teng. Bunday ajratish mas’ul mutaxassisga xizmat nima sababdan yuqori o‘rinni egallaganini tushuntirish imkonini beradi. Indeks hujum ehtimoli yoki tiklanish muvaffaqiyati foizi sifatida talqin qilinmaydi.

Shartli ssenariyda to‘lov tizimi uchun RTO 2 soat va RPO 15 daqiqa, ombor hisobi uchun mos ravishda 8 soat va 2 soat, kadrlar xizmati uchun 24 soat va 12 soat deb olinishi mumkin. Bu qiymatlar haqiqiy tashkilotdan olingan o‘lchovlar emas. Ular ustuvorlik bahosi bilan tiklash talablarining farqini ko‘rsatadi: yuqori indeks xizmatning muhimligini bildirsa, RTO tiklash uchun maqsadli muddatni, RPO esa ma’lumot yo‘qotishining maqbul vaqt oralig‘ini belgilaydi.

Model qaror sabablarini alohida indikatorlar orqali izohlash imkonini beradi. Ekspert bahosining subyektivligi, monitoringdagi noto‘g‘ri signallar va tiklash guruhlari sig‘imi natijaga ta’sir qilishi mumkin. Keyingi sinovlarda ekspert qarori bilan moslik, RTO cheklovlari buzilishi ulushi hamda vaznlar o‘zgarishiga sezgirlik baholanishi kerak. Keltirilgan hisoblash real tajriba natijasi emas.

Koeffitsiyentlarning barqarorligini tekshirishda ularning yig‘indisi birga tengligi saqlanib, ayrim vaznlar o‘zgartiriladi va xizmatlar reytingi qayta hisoblanadi. Kichik o‘zgarishlar natijasida tartib keskin almashsa, qaror ekspertlar bilan qayta muhokama

qilinishi kerak. Bank, ta’lim yoki ishlab chiqarish tashkilotlari uchun bir xil vaznlarni avtomatik qo‘llash maqsadga muvofiq emas. Keyingi tadqiqotlarda taklif etilgan modelni oldindan belgilangan tiklash ro‘yxati va ekspertlar qarori bilan bir xil ssenariylarda taqqoslash rejalashtirilishi mumkin.

Xulosa

BIA, kiberxavf, xizmatlararo bog‘liqlik va anomaliya signalini birlashtiruvchi gibrid model tiklanish ustuvorligini asoslash uchun taklif etildi. RTO, RPO va MTPD talablarini mustaqil cheklov sifatida qo‘llash rejaning bajarilishini tekshirishga xizmat qiladi. Modelning amaliy samaradorligini tasdiqlash uchun real yoki nazorat ostidagi sinovlar va monitoring indikatorlarini kalibrlash talab etiladi.

Joriy etishda jarayonlar reyestri, yagona baholash shkalasi va bog‘liqliklar aniqlashtiriladi. Model nazorat ostidagi ssenariylarda ekspertlar qarori bilan solishtirilishi kerak. Tiklash vaqtining qisqarishi yoki yo‘qotishlarning kamayishi hozircha tajribada isbotlangan natija sifatida da’vo qilinmaydi.

Foydalanilgan adabiyotlar

1. Bartock, M., Cichonski, J., Souppaya, M., Smith, M., Witte, G., & Scarfone, K. (2016). *Guide for cybersecurity event recovery (NIST Special Publication 800-184). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-184*
2. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), Article 15. https://doi.org/10.1145/1541880.1541882
3. G‘aniyev, S. K., G‘aniyev, A. A., & Xudoyqulov, Z. T. (2021). *Kiberxavfsizlik asoslari.* Iqtisod-Moliya.
4. G‘ulomov, Sh. R., Botirov, F. B., & Azizova, Z. I. (2021). *Hujum insidentlari va unga reaksiya.* Mahalla va oila.

5. G‘ulomov, Sh. R., Nasrullayev, N. B., Shirinov, L. T., & Sayfullayev, Sh. B. (2024*). Axborot tizimlari auditi.* Metodist.
6. International Organization for Standardization. (2018). *ISO 31000:2018 risk management—Guidelines. https://www.iso.org/standard/31000*
7. International Organization for Standardization. (2019). *ISO 22301:2019 security and resilience—Business continuity management systems—Requirements. https://www.iso.org/standard/75106.html*
8. International Organization for Standardization. (2020). *ISO 22313:2020 security and resilience—Business continuity management systems—Guidance on the use of ISO 22301. https://www.iso.org/standard/75107.html*
9. Swanson, M., Bowen, P., Phillips, A., Gallup, D., & Lynes, D. (2010). *Contingency planning guide for federal information systems (NIST Special Publication 800-34 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-34r1*
10. Tabassi, E. (2023). Artificial intelligence risk management framework (AI RMF 1.0) (NIST AI 100-1). *National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.100-1*