AXBOROT XAVFSIZLIGIDA RISK TURLAR VA ULARNING TAHLIL USULLARI.

Raxmatullayev Doston Asad o‘g‘li
Qarshi davlat texnika universiteti assistenti
e-mail:nasdaqdoston@gmail.com

Annotatsiya. Axborot xavfsizligi – bu ma’lumotlarning maxfiyligi, yaxlitligi va mavjudligini himoya qilish jarayoni. Har bir tashkilotda ma’lumotlar xavfsizligini baholash uchun risk tahlili olib boriladi. Ushbu maqolada axborot xavfsizligidagi asosiy risk turlari va ularni tahlil qilish usullari ko‘rib chiqiladi.

Kalit so‘zlar: Axborot xavfsizligi, Ma’lumotlar bazasi, IoT (Internet of Things), Ochiq kodli operatsion tizimlar.

TYPES OF RISK IN INFORMATION SECURITY AND METHODS OF THEIR ANALYSIS.

Raxmatullayev Doston Asad o‘g‘li
Qarshi State Technical University assistant
e-mail:nasdaqdoston@gmail.com

Abstract: Information security is the process of protecting the confidentiality, integrity and availability of information. Each organization conducts risk analysis to assess data security. This article will consider the main types of risks in information security and methods of their analysis.

Keywords: Information Security, database, IoT (Internet of Things), open source operating systems.

Kirish. Axborot xavfsizligi risklarini tahlil qilish – bu tashkilotning xavfsizlik strategiyasining asosiy qismi hisoblanadi bularga quyidagilar kiradi. **Safatli** va **miqdori** usullar yordamida xavflarni aniqlash, ularni baholash va samarali boshqarish orqali ma’lumotlarni himoya qilish mumkin. Har bir tashkilot o‘zining risk profili asosida mos usullarni tanlashi kerak. Axborot xavfsizligida riskni boshqarish – bu tashkilotning xavflarni aniqlash, baholash va ularga munosabat bildirish jarayonidir. Quyida **4 ta asosiy risk boshqarish strategiyasi** va ularni qo‘llash usullari keltirilgan.

1. Riskni qabul qilish qachon qo‘llaniladi?

- Agar riskning ta’siri past bo‘lsa (masalan, kichik moliyaviy yo‘qotish).
- Riskni bartaraf qilish xarajati uning o‘zidan yuqori bo‘lsa.

Misol: Kichik ofisda printerning vaqti-vaqti bilan ishdan chiqishi (ta’sir past, tuzatish o’rtacha).

2. Riskni kamaytirish usul qo‘llaniladi?

- Risk yuqori darajada xavfli bo‘lsa, lekin uni butunlay bartaraf qilib bo‘lmasa.
- Xavfni ma’qul darajaga tushirish kerak bo‘lsa. Qo’yidagi usullardan foydalanish kerak bo’ladi.

Texnik choralar:

- Firewall, antivirus, IDS/IPS tizimlari.
- Ikki faktorli autentifikatsiya (2FA).
- Ma’lumotlarni shifrlash (Encryption).

Ma’muriy choralar:

- Xodimlarni xavfsizlik bo‘yicha o‘qitish.
- Parol siyosatini joriy etish.
- Muvofiqlik standartlari (ISO 27001, NIST, GDPR).

Fizik himoya:

- Biometrik kirish tizimlari.
- Server xonalariga ruxsatnomalar.

Misol: Tizimga kirishda **parol + SMS-tasdiq** qo‘llash (riskni kamaytiradi).

3. Riskni o‘tkazish qachon qo‘llaniladi?

- Tashkilot riskni o‘zi emas, boshqa tomonga yuklashni xohlasa.
- Sug‘urta yoki uchinchi tomon xizmatlaridan foydalanish.

Usullari:

- Sug‘urta qilish (Cyber Insurance) – ma’lumotlar o‘g‘irlanishi yoki DDoS hujumi uchun.
- Outsourcing – bulut xizmatlariga (AWS, Azure) tayanib, xavfni provayderga yuklash.

Shartnoma shartlari – agar ma’lumotlar uchinchi tomon tomonidan boshqarilsa.

Misol: Kiberxavfsizlik sug‘urtasi (ransomware hujumi ta’sirini kamaytiradi).

4. Riskni bartaraf qilish uchun qo‘llaniladi?

- Risk juda yuqori bo‘lsa va unga yo‘l qo‘yish mumkin bo‘lmasa.
- Faoliyatni butunlay to‘xtatish yoki alternativ yo‘l tanlash.

Usullari:

- Xavfli texnologiyalardan voz kechish (masalan, Windows XP dan foydalanishni to‘xtatish).
- Internetga ulanishni cheklash (maxsus tarmoqlarda ishlash).
- Ma’lumotlarni bulutga joylashmaslik (o‘z serverlarida saqlash).

Misol: Kredit karta ma’lumotlarini cloudda saqlamaslik.

Riskni boshqarish strategiyalari 1-jadval

Strategiya	Qo'llash Shartlari	Misol	Afzalliklari
Qabul qilish	Past xavf, arzimas ta'sir	Printerning ishdan chiqishi	Xarajatni tejash, oddiy yechim
Kamaytirish	Xavfni ma'qul darajaga tushirish	2FA, firewall, shifrlash	Xavfni nazorat ostiga olish
O'tkazish	Boshqa tomonga yuklash	Kiber-sug'urta, bulut xizmatlari	Moliyaviy yukni kamaytirish
Bartaraf etish	Riskni butunlay yo'q qilish	Windows XP dan voz kechish	To'liq xavfsizlikni ta'minlash

Xulosa: Axborot xavfsizligida risklarni samarali boshqarish - bu tashkilotlarning muvaffaqiyatli faoliyati uchun asosiy shart hisoblanadi. Quyidagi to'rtta asosiy strategiya xavflarni nazorat qilishning to'liq doiyasini taqdim etadi. Xulosa qilib aytganda, muvaffaqiyatli risk boshqaruvi - bu faqatgina texnik yechimlar emas, balki tashkilot madaniyatining ajralmas qismidir. Har bir tashkilot o'zining xususiyatlariga mos strategiyalar kombinatsiyasini ishlab chiqishi va uni doimiy ravishda takomillashtirishi kerak.

Foydalanilgan adabiyotlar.

1. Raxmatullayev, D. A., & Sh, N. B. (2025). IOT TIZIMLARIDA ENERGIYA SAMARADORLIGINI OSHIRISH VA ENERGIYA TEJASH IMKONIYATLARI. *Iqtisodiyot va jamiyat*, (1-2 (128)), 1008-1012.
2. Raxmatullayev, D. A., & Sh, N. B. (2025). IOT TIZIMLARIDA ENERGIYA SAMARADORLIGINI OSHIRISH VA ENERGIYA TEJASH IMKONIYATLARI. *Iqtisodiyot va jamiyat*, (1-2 (128)), 1008-1012.
3. **"Risk Management in Cybersecurity"** – Gregory J. Touhill, C. Joseph Touhill (2020)
4. Raxmatullayev, D. A. (2024). AXBOROT XAVFSIZLIGI SOHASIDA TAQSIL OLADIGAN TALABALARNING KEBIR XAVFSIZLIKNI O‘QITISH METODIKASINI TAKOMILLASHTIRISH. TADQIQOTLAR, 30(3), 103-107.
5. **"Best Practices in Cyber Risk Transfer"** – SANS Institute Whitepaper (2023)
6. Uzakov, O. S., Raxmatullayev, D. A., Bekmatov, A. K., & Dilmurodov, Z. D. (2023). IOT TEXNOLIGIYALARI XAVFSIZLIGIDA SMART HOUSELARNI MOBIL QURILMALAR YORDAMIDA BOSHQARISH. ОБРАЗОВАНИЕ НАУКА И ИННОВАЦИОННЫЕ ИДЕИ В МИРЕ, 23(7), 105-107.
7. Эгамбердиев, Ҳ., Рахматуллаев, Д., & Дилмуродов, З. (2023). ГРУНТ ВА ЕР УСТИ СУВ ОҚИМЛАРИНИНГ ЎЗАРО ТАЪСИРИНИНГ МАТЕМАТИК МОДЕЛИ. Евразийский журнал академических исследований, 3(1 Part 3), 107-113.