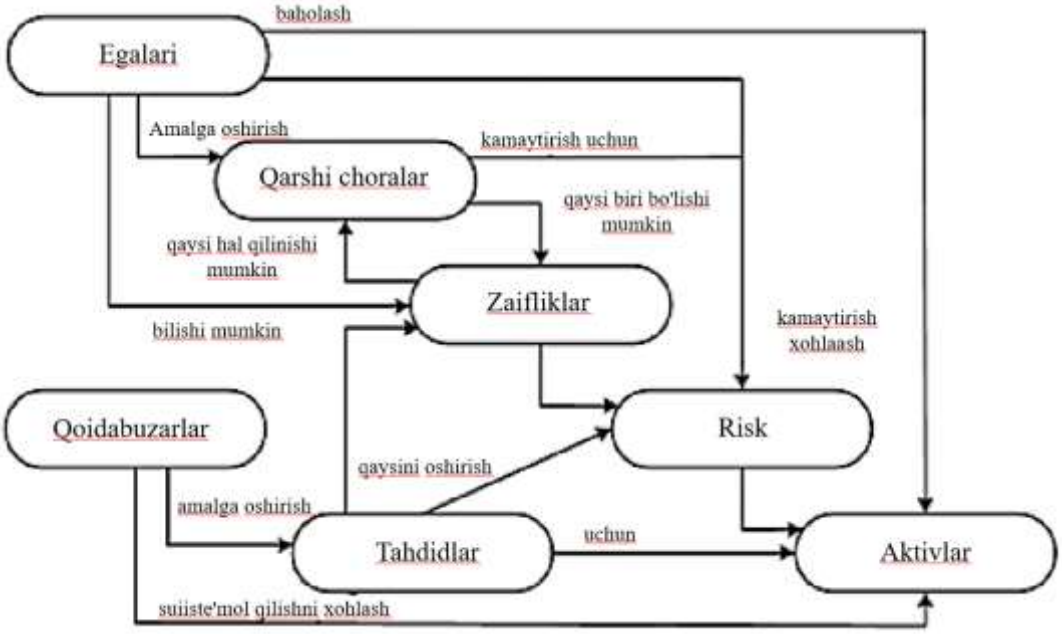
KIBERXAVFSIZLIKDA RISKLARNI BAHOLASHNI TAHLIL QILISH

Polvonov Baxtiyor
Muhammad al-Xorazmiy nomidagi TATU Farg‘ona filiali dotsenti
O‘rinboyev Alisher
Muhammad al-Xorazmiy nomidagi TATU Farg‘ona filiali talabasi

Annotatsiya. *Ushbu maqolada bugungi kunda rivojlanayotgan kiberxavfsizlik sohasida riskni baholash usullarini va axborot tizimini himoya qilish zarurligini o‘rganish haqida ma’lumotlar berilgan. Yuqori sifatli texnikani qo‘llash orqali xavflarni hisoblashni amaliy va nazariy tahlil qilingan.*

Kalit so‘zlar: *xavfsizlik, kiberxavfsizlik, risk, tahdid, razvetka.*

Barcha tahdidlarni hisobga olish kerak, lekin birinchi navbatda tasodifiy va qasddan qilingan insoniy harakatlar bilan bog‘liq. Aktivlarni himoya qilishda ularning egalari manfaatdor. Biroq, bu aktivlar egalari manfaatlariga zid ravishda o‘z maqsadlari uchun aktivlardan foydalanishga intilayotgan jinoyatchilar uchun ham qiziqish uyg‘otadi. Xavfsizlik buzilishi odatda (faqat ushbu toifalar bilan cheklanmagan): ruxsatsiz oshkor qilish (maxfiylikni yo‘qotish), ruxsat etilmagan modifikatsiya (yaxlitlikni yo‘qotish) yoki aktivlarga ruxsatsiz kirishdan mahrum qilish (mavjudlik yo‘qolishi).



1 -rasm - Xavfsizlik kontseptual tushunchalari sxemasi va ularning o‘zaro bog‘liqligi.

Aktiv egalari riskni tahlil qilishlari kerak, ya’ni. tahdidlarni, zaif joylarni, har bir tahdidni va qarshi choralarni amalga oshirishdan mumkin bo‘lgan zararni aniqlash. Mulk egasi tomonidan talab qilinadigan aktivlar xavfsizligi siyosatini amalga oshirish uchun, buzg‘unchilar ularni ishlatishi mumkinligi sababli, zaifliklar sonini kamaytirish uchun choralar ko‘rish kerak.

Tizim (mahsulot) ishga tushirilishidan oldin ham AT egasi tahdidlarga qarshi choralar samaradorligini baholashdan manfaatdordir. Bunday baholashning natijasi-qarshi choralar aktivlar uchun riksni kamaytiradigan kafolat darajasi to‘g‘risida xulosa. Kafolat AT tizimining (mahsulot) xavfsizlik muammolariga javob berishiga ishonch hosil qilish uchun asoslidir.

Sifatli metodologiya umumiy va maxsus baholashlarni o‘tkazish uchun mo‘ljallangan bo‘lib, bu tashkilot rahbariga kelajakda himoya xarajatlarini baholab, tashkilot ichida aylanayotgan maxfiy ma’lumotlarni raqobatchilardan himoya qilish zarurligi to‘g‘risida asosli qaror qabul qilish imkonini beradi. Texnika sizga maxfiy ma’lumotlarni himoya qilish zarurligini tezkor va adolatli baholashga imkon beradi va shu asosda tezda tegishli qarorni qabul qiladi, ya’ni rahbarga katta tijorat muvaffaqiyatsizliklari va foyda yo‘qotishdan saqlanish imkonini beradi. raqobatchilar uchun ma’lumotlarning mavjudligi.

Tashkilot ichida aylanayotgan maxfiy ma’lumotlarni himoya qilish zarurligi to‘g‘risida qaror tashkilot rahbariyati tomonidan qabul qilinishi kerak. Hech kim menejment, tashkilot sirlarini himoya qilish kabi choralarga qiziqmaydi va hech kim tashkilotda aylanayotgan ma’lumotlarning butun majmuasini, uning maxfiylik darajasini, ichki va tashqi holatini, uning asoschisi sifatida bilmaydi.

Texnika ikkita o‘zaro bog‘liq qismdan iborat. Birinchi qism, so‘rov natijalarini qayta ishlash asosida, tashkilotda aylanayotgan ma’lumotlarni himoya qilish kerakmi yoki yo‘qmi degan savolga, ikkinchi qismi esa, agar ijobiy hal qilingan bo‘lsa, javob berishga imkon beradi. Birinchi savol, yaqinlashib kelayotgan axborotni himoya qilish xarajatlarini taxminiy baholash imkonini beradi.

Tashkilot asoschisining qiziqishi, malakasi va dunyoqarashini hisobga olgan holda, iloji boricha tashkilot asoschisining bilimlari, tajribasi va fikrini hisobga oladigan usul taklif etiladi. Metodologiyaning birinchi qismi keyinchalik uning natijalarini qayta ishlash bilan anketa so‘rovi usuliga asoslangan.

Bu usulni amalga oshirish uchun tashkilot asoschisi uchun tashkilot faoliyatining unda aylanayotgan ma’lumotlar bilan bog‘liq barcha jihatlarini qamrab oladigan so‘rovnomalar savollari ro‘yxati ishlab chiqilgan.

Anketa savollari shunday tuzilganki, ular uzoq javoblarni talab qilmaydi, balki "ha", "yo‘q" munosib javoblarga aylanadi. Anketani to‘ldirish axborot xavfsizligi sohasida maxsus tayyorgarlikni talab qilmaydi va qiyinchilik va ko‘p vaqt talab qilmaydi. Anketa savollarini ishlab chiqishda va keyinchalik axborot xavfsizligi bo‘yicha mutaxassislar ishtirokida so‘rov natijalarini qayta ishlashda axborot xavfsizligi bo‘yicha maxsus bilimlar hisobga olingan.

Anketa savollariga berilgan javoblarni matematik tarzda qayta ishlash orqali holat va qo‘shimcha himoya zarurligiga miqdoriy baho olinadi. Shu maqsadda, anketaning har bir savoliga maxfiy ma’lumotlarni himoya qilishning umumiy tizimiga qo‘shgan hissasini raqamli ifodalovchi og‘irlik qiymati beriladi. Og‘irlik koeffitsientlarining qiymatlari ekspert usuli bilan olingan.

Anketa natijalarini qayta ishlashda siz tashkilotdagi himoya holatining umumiy bahosini ham, himoya sohalarida bir qator shaxsiy baholarni ham olishingiz mumkin. Barcha baholar yig‘indisi menejerga, oxir -oqibat, xavfsizlik, tashkiliy va texnik tadbirlarni o‘tkazish orqali himoyani tashkil etish zarurligi to‘g‘risida qaror qabul qilishga imkon beradi. Himoyalashning har bir komponenti bahosini tahlil qilish asosida, axborot himoyasi ta’minlanmagan va raqobatchining uni ushlab qolish ehtimoli (oqish) qabul qilinmaydigan darajada yuqori bo‘lgan havolalar aniqlanadi. Bunday tahlilni o‘tkazgandan so‘ng, tashkilot rahbari maqsadli ravishda aniqlangan sohalarda axborot oqishini bartaraf etish ishlarini olib borishi mumkin.

Foydalanilgan adabiyotlar.

1. Muxtarov, F., & Sadirova, X. (2023). Korxonada axborot xavfsizligini ta'minlashning zamonaviy usullari. *Engineering problems and innovations*.
2. Nabijonov, R., & Ergasheva, A. (2023). Masofaviy o'qitish tizimlarini ta'lim sifatini oshirishdagi o'rni. *Engineering Problems and Innovations*. извлечено от https://fer-teach.uz/index.php/epai/article/view/44
3. Muxtarov, F., & Tojidinov , A. (2023). Tarmoq xavfsizligini url filtirlash bilan yaxshilash. *Research and Implementation*, *1*(4), 39–44. извлечено от https://fer-teach.uz/index.php/rai/article/view/890
4. Nabijonov Ravshanbek Muxammadjon o'g'li. (2022). Media portal yaratishning asosiy afzallik va kamchiliklarI . *World Scientific Research Journal*, *10*(2), 125–131. Retrieved from http://wsrjournal.com/index.php/wsrj/article/view/2379
5. Nabijonov Ravshanbek Muxammadjon o'g'li, Azamov Shohruhmirzo Alisher o'g'li, & Ergasheva Asaloy Dilmurod qizi. (2022). TRACE MODE texnologiyasi. *Proceedings of International Conference on Educational Discoveries and Humanities*, *1*(2), 106–112. Retrieved from https://econferenceseries.com/index.php/icedh/article/view/246
6. Muxammadjon o'g'li, N. R., Mavlonjon o'g, M. J. M., & Erali o'g, T. Y. A. (2022). Tibbiyotda qo'llanadigan zamonaviy kompyuter tizimlari klassifikatsiyasi.
7. Nabijonov , R., Ergasheva , A., Ibrohimova , N., & Azamov , S. (2023). Masofaviy ta'limda internet tizimlari afzalliklari va ulardan xavfsiz foydalanish usullari. Research and Implementation, 1(4), 31–38. извлечено от https://fer-teach.uz/index.php/rai/article/view/881
8. Nabijonov , R., Azamov , S., Ergasheva , A., & Ibrohimova , N. (2023). Biznesni avtomatlashtirishning bugungi kundagi ahamiyati. Research and Implementation, 1(4), 16–24. извлечено от https://fer-teach.uz/index.php/rai/article/view/879

9. Nabijonov , R., Ibrohimova , N., Azamov , S., & Ergasheva , A. (2023). Bulutli texnologiyalar tizimida axborot xavfsizligi. Research and Implementation, 1(3). извлечено от https://fer-teach.uz/index.php/rai/article/view/877

10. Nabijonov , R., & Azamov , S. (2023). Kompyuter tarmoqlariga tahdid qiluvchi masofaviy hujumlar tahlili. Engineering Problems and Innovations. извлечено от https://fer-teach.uz/index.php/epai/article/view/884

11. Nabijonov , R., & Ibrohimova , N. (2023). Flutter frameworkidan foydalnishning afzalliklari va kamchiliklari. Engineering Problems and Innovations. извлечено от https://fer-teach.uz/index.php/epai/article/view/883

12. Nabijonov , R., & Rasulov , A. (2023). Zamonaviy media portal imkoniyatlaridan unumli foydalanish. *Research and Implementation*. извлечено от https://fer-teach.uz/index.php/rai/article/view/767

13. Xonto‘rayev, S. (2023). Oliy ta’lim muassasalarida Web resurslarda mavjud dasturiy, texnik va uslubiy muammolarni bartaraf etish. Scientific-technical journal (STJ FerPI, ФарПИ ИТЖ, НТЖ ФерПИ, 2023, Т. 27. спец. выпуск№ 2).

14. Обухов, В., Ходжиматов Ж., & Набижонов , Р. (2023). Развитие блокчейн технологий в узбекистане: современные вызовы и перспективы. *Research and Implementation*. извлечено от https://fer-teach.uz/index.php/rai/article/view/768