# KIBERXAVFSIZLIK: TIZIMLAR, TARMOQLAR VA MAXFIY MA'LUMOTLARNI RUXSATSIZ KIRISH, FOYDALANISH, OSHKOR QILISH, BUZISH, O'ZGARTIRISH YOKI YO'Q QILISHDAN HIMOYA QİLİSH.

**Xurramov Ruslan Erkin o'g'li**
ruslanxurramov852@gmail.com
Termiz davlat universiteti
Axborot texnologiyalari kafedrasi o'qituvchisi

***Annotatsiya.*** *Ushbu mavzu kompyuter tizimlari, tarmoqlar, dasturiy ta'minot va ma'lumotlar kabi axborot texnologiyalari (IT) aktivlarini kiber tahdidlardan himoya qilishni nazarda tutadi. Kiber tahdidlar turli shakllarda bo'lishi mumkin, jumladan viruslar, zararli dasturlar, fishing hujumlari, to'lov dasturi, ijtimoiy muhandislik va insayder tahdidlar. Kiberxavfsizlik ushbu tahdidlarning IT aktivlarining maxfiyligi, yaxlitligi va mavjudligini buzishining oldini olishga qaratilgan. Bu AT aktivlarini ruxsatsiz kirish, foydalanish, oshkor qilish, buzish, o'zgartirish yoki yo'q qilishdan himoya qilishni ta'minlash uchun bir qator amaliyotlar, texnologiyalar va siyosatlarni amalga oshirishni o'z ichiga oladi. Samarali kiberxavfsizlik choralari jismoniy shaxslar, tashkilotlar va hukumatlar uchun kiberhujumlardan himoyalanish hamda ma'lumotlarning buzilishi, moliyaviy yo'qotishlar va obro'ga putur yetkazish xavfini minimallashtirish uchun zarurdir.*

***Kalit so'zlar.*** *Kiberxavfsizlik, himoya, tizimlar, tarmoqlar, maxfiy ma'lumotlar, ruxsatsiz kirish, foydalanish, oshkor qilish, buzish, o'zgartirish, yo'q qilish, kiber tahdidlar, viruslar, zararli dasturlar, fishing hujumlari, to'lov dasturi, ijtimoiy muhandislik, insayder tahdidlar, maxfiylik, yaxlitlik, mavjudlik, amaliyotlar, texnologiyalar, siyosatlar, ma'lumotlarning buzilishi, moliyaviy yo'qotishlar, obro'ga zarar.*

**Kirish.** Axborot xavfsizligi muhim ma'lumotlar saqlanadigan, qayta ishlanadigan va elektron shaklda uzatiladigan bugungi raqamli asrda juda muhim muammodir. Zararli dasturlar, fishing hujumlari va ma'lumotlarning buzilishi kabi kibertahdidlarning ko'payishi axborot xavfsizligini ta'minlash bo'yicha samarali choralar ko'rish zarurligini ta'kidladi. Axborot xavfsizligi axborotning maxfiyligi, yaxlitligi va mavjudligini, shuningdek, ularni qayta ishlovchi va saqlaydigan AT aktivlari, tizimlari va tarmoqlarini himoya qilishga qaratilgan. Bu axborot va AT

aktivlarini ruxsatsiz kirish, foydalanish, oshkor qilish, buzish, o‘zgartirish yoki yo‘q qilishdan himoya qilishni ta’minlash uchun amaliyotlar, texnologiyalar va siyosatlar to‘plamini amalga oshirishni o‘z ichiga oladi. Bunga xavfsizlik devorlari, shifrlash, kirishni boshqarish vositalari, hodisalarga javob berish rejalari va xodimlar uchun xavfsizlik bo‘yicha treninglar kabi choralar kiradi. Samarali axborot xavfsizligi jismoniy shaxslar, tashkilotlar va hukumatlar uchun kiberhujumlardan himoya qilish va maxfiy ma’lumotlarni ma’lumotlar buzilishi, moliyaviy yo‘qotishlar va obro‘ga putur etkazishdan himoya qilish uchun juda muhimdir.

**Adabiyotlar tahlili.** Axborot xavfsizligi bo‘yicha adabiyotlar tahlili keng va doimiy rivojlanib boruvchi sohani qamrab oladi, biroq ba’zi umumiy mavzular va tendentsiyalarni aniqlash mumkin.

Axborot xavfsizligiga kompleks va kompleks yondashuvning ahamiyati diqqat markazida bo‘ladi. Bu nafaqat xavfsizlik devorlari va shifrlash kabi texnik choralarni, balki siyosatlar, protseduralar va xodimlarni o‘qitish kabi texnik bo‘lmagan omillarni ham o‘z ichiga oladi. Axborot xavfsizligining samarali ta’minlanishi tashkilotning barcha jihatlarini, ya’ni qo‘llanilayotgan texnologiyadan tortib, undan foydalanadigan odamlargacha qamrab oluvchi yaxlit yondashuvni talab qiladi.

Yana bir asosiy mavzu - axborot xavfsizligi sohasida risklarni boshqarish zarurati. Xavflarni boshqarish potentsial tahdidlar va zaifliklarni aniqlash va baholashni, ularning ehtimoli va potentsial ta’siridan kelib chiqqan holda ustuvorlikni belgilashni va tegishli choralarni ko‘rishni o‘z ichiga oladi. Ushbu yondashuv tashkilotlarga o‘z kuchlarini eng muhim xavflarga qaratishga va resurslarni samarali taqsimlashga yordam beradi.

So‘nggi yillarda bulutli hisoblash va mobil qurilmalarning yuksalishi axborot xavfsizligi uchun yangi muammolar va imkoniyatlarni keltirib chiqardi. Bulutli hisoblash kengaytirilgan miqyoslilik va moslashuvchanlik kabi ko‘plab afzalliklarni taqdim etadi, ammo u ma’lumotlarning buzilishi va kiber hujumlar kabi yangi xavfsizlik xavflarini ham taqdim etadi. Xuddi shunday, mobil qurilmalar ham unumdorlik va hamkorlik uchun ko‘plab afzalliklarni taqdim etadi, ammo ular to‘g‘ri himoyalanmagan bo‘lsa, hujumlar va ma’lumotlar yo‘qotilishiga qarshi himoyasiz bo‘lishi mumkin.

Va nihoyat, axborot xavfsizligini ta’minlashda hamkorlik va ma’lumot almashishning ahamiyati tobora ortib bormoqda. Kibertahdidlar tobora murakkablashib, keng tarqalmoqda va hech bir tashkilot yakka holda ishlashga qodir emas. Tahdidlar, zaifliklar va ilg‘or amaliyotlar haqidagi ma’lumotlarni almashish tashkilotlarga paydo bo‘ladigan xavflardan oldinda bo‘lishga va o‘z aktivlarini yaxshiroq himoya qilishga yordam beradi.

Umuman olganda, axborot xavfsizligi bo‘yicha adabiyotlar tahlili tashkilotning barcha jihatlarini qamrab oluvchi hamda paydo bo‘ladigan tahdidlardan oldinda turish uchun hamkorlik va ma’lumot almashishni qo‘llaydigan yaxlit va xavfga asoslangan yondashuv zarurligini ta’kidlaydi.

**Tadqiqot metodologiyasi.** Axborot xavfsizligini tadqiq qilish metodologiyasi aniq tadqiqot savoliga qarab farq qilishi mumkin, ammo ba’zi umumiy yondashuvlar quyidagilarni o‘z ichiga oladi:

Adabiyotlarni ko‘rib chiqish: Tegishli nazariyalar, asoslar, tushunchalar va ilg‘or tajribalarni aniqlash uchun mavzu bo‘yicha mavjud adabiyotlarni har tomonlama ko‘rib chiqish.

Vaziyatni o‘rganish: Axborot xavfsizligi buzilishi va hodisalarining haqiqiy misollarini tahlil qilish, umumiy naqshlar, sabablar va oqibatlarni aniqlash va samarali kamaytirish strategiyalarini aniqlash.

So‘rovlar: shaxslar yoki tashkilotlardan ularning axborot xavfsizligi bilan bog‘liq tushunchalari, munosabati va xatti-harakatlari bo‘yicha ma’lumotlarni to‘plash. Bu xodimlar, mijozlar yoki soha mutaxassislari so‘rovlarini o‘z ichiga olishi mumkin.

Suhbatlar: Axborot xavfsizligi bo‘yicha mutaxassislar, rahbarlar yoki tartibga soluvchilar kabi asosiy manfaatdor tomonlar bilan ularning axborot xavfsizligi bo‘yicha qarashlari haqida tushunchaga ega bo‘lish uchun chuqur suhbatlar o‘tkazish.

Kuzatishlar: odamlar texnologiyadan qanday foydalanishi va nozik ma’lumotlarni qanday himoya qilishlari haqida tushunchaga ega bo‘lish uchun ish joyi yoki jamoat joylari kabi real sharoitlarda axborot xavfsizligi amaliyotlarini kuzatish.

Tajribalar: Axborot xavfsizligi choralari yoki aralashuvi samaradorligini tekshirish uchun nazorat ostida tajribalar o‘tkazish.

Aralash usullar: Axborot xavfsizligi masalalarini yanada kengroq tushunish uchun so‘rovlar va amaliy tadqiqotlar kabi bir nechta usullarni birlashtirish.

Umuman olganda, axborot xavfsizligini tadqiq qilish metodologiyasi qat’iy, tizimli va tadqiqot savoliga mos bo‘lishi kerak. Shuningdek, u ishtirokchilarning shaxsiy hayoti va maxfiyligini himoya qilish va tadqiqot natijalari axloqiy va mas’uliyatli tarzda tarqatilishini ta’minlash kabi axloqiy jihatlarni hisobga olishi kerak.

**Tahlil va natijalar.** Axborot xavfsizligi bo‘yicha tadqiqotlar tahlili va natijalari qo‘llaniladigan metodologiyaga va aniq tadqiqot savoliga qarab farq qilishi mumkin. Biroq, axborot xavfsizligi bo‘yicha tadqiqotlarning ba’zi umumiy topilmalari quyidagilarni o‘z ichiga oladi:

Axborot xavfsizligiga kompleks va kompleks yondashuvning ahamiyati. Samarali axborot xavfsizligi nafaqat xavfsizlik devori va shifrlash kabi texnik

choralarni, balki siyosat, protseduralar va xodimlarni o‘qitish kabi texnik bo‘lmagan omillarni ham talab qiladi.

Axborot xavfsizligida risklarni boshqarish zarurati. Xavflarni boshqarish potentsial tahdidlar va zaifliklarni aniqlash va baholashni, ularning ehtimoli va potentsial ta’siridan kelib chiqqan holda ustuvorlikni belgilashni va tegishli choralarni ko‘rishni o‘z ichiga oladi.

Axborot xavfsizligini ta’minlashda hamkorlik va axborot almashishning ahamiyati. Kibertahdidlar tobora murakkablashib, keng tarqalmoqda va hech bir tashkilot yakka holda ishlashga qodir emas. Tahdidlar, zaifliklar va ilg‘or amaliyotlar haqidagi ma’lumotlarni almashish tashkilotlarga paydo bo‘ladigan xavflardan oldinda bo‘lishga va o‘z aktivlarini yaxshiroq himoya qilishga yordam beradi.

Axborot xavfsizligida bulutli hisoblash va mobil qurilmalarning ahamiyati ortib bormoqda. Bulutli hisoblash va mobil qurilmalar samaradorlik va hamkorlik uchun ko‘plab afzalliklarni taklif qiladi, lekin ma’lumotlarning buzilishi va kiberhujumlar kabi yangi xavfsizlik xavflarini ham keltirib chiqarishi mumkin.

Axborot xavfsizligiga inson omillarining ta’siri. Texnik choralar muhim bo‘lsa-da, xodimlarning xatti-harakati va xabardorligi kabi inson omillari ham axborot xavfsizligiga sezilarli ta’sir ko‘rsatishi mumkin. Samarali axborot xavfsizligi nafaqat texnik choralarni, balki yaxshi xavfsizlik amaliyotlarini qadrlaydigan va targ‘ib qiluvchi xavfsizlik madaniyatini ham talab qiladi.

Umuman olganda, axborot xavfsizligi bo‘yicha tadqiqotlar tahlili va natijalari tashkilot faoliyatining barcha jihatlarini qamrab oluvchi, hamkorlik va ma’lumot almashishni qo‘llaydigan hamda inson omillarining xavfsizlikka ta’sirini hisobga oladigan yaxlit va xavfga asoslangan yondashuvning muhimligini ta’kidlaydi. Topilmalar paydo bo‘ladigan tahdidlardan himoya qiluvchi va ma’lumotlarning buzilishi, moliyaviy yo‘qotishlar va obro‘ga putur etkazish xavfini minimallashtiradigan samarali axborot xavfsizligi strategiyalari va amaliyotlarini ishlab chiqishda foydalanish mumkin.

## Xulosa

Xulosa qilib aytadigan bo‘lsak, axborot xavfsizligi alohida shaxslar, tashkilotlar va butun jamiyatga ta’sir qiluvchi muhim masaladir. Raqamli texnologiyalar, bulutli hisoblash va mobil qurilmalarga tobora ortib borayotgan ishonch xavfsizlikka yangi xavf va muammolarni keltirib chiqardi, bu esa samarali axborot xavfsizligini har qachongidan ham muhimroq qiladi. Axborot xavfsizligi bo‘yicha adabiyotlar tahlili tashkilotning barcha jihatlarini, shu jumladan siyosat, protseduralar va xodimlarni o‘qitishni o‘z ichiga olgan keng qamrovli va integratsiyalashgan yondashuvning muhimligini ta’kidlaydi. Xatarlarni boshqarish ham muhim ahamiyatga ega, chunki u

tashkilotlarga potentsial tahdidlar va zaifliklarni birinchi o‘ringa qo‘yish va yumshatishga yordam beradi. Hamkorlik va ma’lumot almashish paydo bo‘layotgan tahdidlardan oldinda turish uchun muhim ahamiyatga ega va inson omillarining axborot xavfsizligiga ta’sirini e’tiborsiz qoldirib bo‘lmaydi. Axborot xavfsizligi bo‘yicha tadqiqotlar tahlili va natijalari kibertahdidlardan himoyalanish hamda ma’lumotlarning buzilishi, moliyaviy yo‘qotishlar va obro‘ga putur yetkazish xavfini minimallashtirish bo‘yicha samarali strategiya va amaliyotlar haqida qimmatli tushunchalar beradi. Oldinga qarab, tashkilotlar axborot xavfsizligiga sarmoya kiritishda davom etishi va eng so‘nggi ilg‘or tajribalar va paydo bo‘layotgan tahdidlardan xabardor bo‘lib turishi zarur.

## FOYDALANILGAN ADABIYOTLAR

1. Whitman, M. E., & Mattord, H. J. (2019). Principles of information security. Cengage Learning.
2. Anderson, R., & Moore, T. (2009). The economics of information security. Science, 314(5799), 610-613.
3. Clarke, R. (1999). Internet privacy concerns confirm the case for intervention. Communications of the ACM, 42(2), 60-67.
4. Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. WW Norton & Company.
5. NIST Cybersecurity Framework. (2018). National Institute of Standards and Technology.
6. ISO/IEC 27001:2013. Information technology - Security techniques - Information security management systems - Requirements.
7. European Union Agency for Cybersecurity (ENISA). (2018). Cybersecurity Culture in Organizations.
8. D’Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. Information Systems Research, 20(1), 79-98.
9. Lee, J., Lee, M., & Lee, I. (2014). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Business Horizons, 57(4), 431-440.
10. Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. MIS Quarterly, 34(3), 487-502.