Vol. 1 No. 3 (2024): Journal of International science networks
Journal of Contemporary World Studies: ISSN: 3030-3311
International Journal of Scientific and Applied Research

AXBOROT XAVFSIZLIGIDA ETIK MASALALAR: MUAMMOLAR VA ULARNI HAL QILISH YO‘LLARI

Karimberganov Timur Alisher o‘g‘li

Abstract: *Ushbu maqola axborot xavfsizligi va etik masalalar o‘rtasidagi muammolarni ko‘rib chiqadi. Shaxsiy ma'lumotlarni himoya qilish, kiberhujumlar, texnologiyalarning adolatsiz foydalanganligi kabi masalalar axborot xavfsizligi doirasidagi etik masalalarga misol keltirilgan. Maqola axborot xavfsizligi sohasida etik muammolarni hal qilish uchun zaruriy strategiyalarni va yechimlarni tahlil qiladi.*

Keywords: *axborot xavfsizligi, etik masalalar, xususiylik, shaxsiy ma'lumotlar, kiberhujumlar, axborot himoyasi, axloqiy kodekslar, ma'lumotlarni yig‘ish va qayta ishlash .*

E-mail: karimberganovtimurbek@gmail.com

Author information: *Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universiteti Jizzax filiali Amaliy matematika fakulteti Axborot xavfsizligi yo‘nalishi 181-23 guruh 2-bosqich talabasi*

1. Kirish

Axborot xavfsizligi sohasidagi etik masalalar bugungi raqamli jamiyatda tobora muhim ahamiyatga ega bo‘lib, ular jamiyatning raqamli infrastrukturasi va shaxsiy axborotlariga zarar yetkazilishi mumkin bo‘lgan xavflar bilan bevosita bog‘liqdir. Shaxsiy ma'lumotlarni himoya qilish, xususiylik huquqlari, axborotlar bilan aloqalar va boshqa xavfsizlik muammolari etika sohasida o‘ziga xos muammolarni keltirib chiqaradi. Axborot xavfsizligi va etika o‘rtasidagi muvozanatni topish, barcha texnologik tizimlar uchun zaruriy asos hisoblanadi, chunki ularning samarali ishlashi nafaqat texnik nuqtai nazardan, balki ijtimoiy va axloqiy jihatdan ham muhimdir.

Ushbu maqolada axborot xavfsizligi va etik masalalar o‘rtasidagi bog‘liqlik, bu masalalarning asosiy muammolari va ularni hal qilish yo‘llari muhokama qilinadi. Etik masalalarni ko‘rib chiqishda, axborot xavfsizligini ta'minlashda ishtirok etuvchi barcha tomonlar – davlatlar, kompaniyalar va foydalanuvchilar – o‘z mas'uliyatlarini qanday anglashlari kerakligi, shuningdek, axborot xavfsizligi sohasidagi innovatsion yondashuvlar va tartib-qoida choralari haqida gapiriladi.

2. Axborot xavfsizligida etik muammolar

2.1. Shaxsiy xavfsizlik va xususiylik

Shaxsiy axborotlarning xavfsizligi va xususiyligi – axborot xavfsizligining eng dolzarb etik masalalaridan biridir. Bugungi kunda foydalanuvchilarning internetda amalga oshirgan barcha faoliyatlari, jumladan, onlayn xaridlar, so‘rovlar, ijtimoiy tarmoqlarda fikrlar va shaxsiy ma'lumotlar, to‘planib, saqlanadi. Bunday ma'lumotlarning nohaq qo‘lga kirishi yoki tijorat maqsadlarida ishlatilishi xususiylik huquqlarini buzish deb hisoblanadi.

Axborot xavfsizligini ta'minlashda kompaniyalar, shuningdek, foydalanuvchilarning shaxsiy ma'lumotlarini qanday saqlash va ishlatishlarini hal qilishda axloqiy mas'uliyatga ega bo‘lishlari kerak. Shaxsiy ma'lumotlarni yig‘ish va ularni anonim tarzda ishlatish bilan bog‘liq etik masalalar juda muhimdir. Foydalanuvchilarga o‘z ma'lumotlari ustidan nazorat berish, ya'ni ular haqida qanday axborot to‘planayotganligi haqida aniq va oshkora ma'lumot berish, bu masalani hal qilishning birinchi qadamidir.

2.2. Axborotlarni yig‘ish va qayta ishlash

Axborot yig‘ish va qayta ishlash jarayonlari ko‘pincha etik muammolarni keltirib chiqaradi. Kompaniyalar foydalanuvchilardan ma'lumotlarni olishda ko‘plab shakllardan foydalanadi, ammo bu ma'lumotlar maxfiyligini buzadigan yoki nohaq foydalanishga olib keladigan holatlar mavjud. Misol uchun, reklamalar yoki shaxsiylashtirilgan xizmatlar uchun yig‘ilayotgan ma'lumotlar foydalanuvchilarni manipulyatsiya qilishga olib kelishi mumkin.

Bundan tashqari, ma'lumotlar bazalarining himoya qilinmasligi yoki nohaq qo‘lga kirishi, shaxsiy ma'lumotlarning o‘g‘irlanishi va noqonuniy ishlatilishi etik muammolarni yanada kuchaytiradi. Bu holatlar, ayniqsa, sog‘liqni saqlash, moliya, va ta'lim kabi sohalarda ko‘proq uchraydi.

2.3. Kiberhujumlar va xavfsizlikni buzish

Kiberhujumlar – bu kompyuter tizimlari va tarmoqlariga noqonuniy kirish, ulardan foydalanish yoki zarar etkazish harakatlaridir. Bu harakatlar, axborot xavfsizligining asosiy etik prinsiplari, ya'ni axborotni himoya qilish, uning yaxlitligi va mavjudligini saqlashga zid keladi. Kiberhujumlar orqali tizimlarga zarar yetkazish, shaxsiy ma'lumotlarni o‘g‘irlash yoki maqsadli kiberhujumlar (masalan, do‘stona davlatlar yoki tashkilotlar ustidan yuritiladigan hujumlar) nafaqat texnik nuqtai nazardan, balki etik jihatdan ham xavfli bo‘ladi.

Hujumlar natijasida yuzaga kelgan ma'lumotlarning yo‘qolishi yoki zarar ko‘rgan foydalanuvchilar bu muammolarni hal qilishda qanday huquqlarga ega ekanligini aniqlash kerak. Bu, axborot xavfsizligi va etik xatarlarga qarshi kurashishda huquqiy choralarning qanday bo‘lishi kerakligini o‘ylab topish zarurati tug‘diradi.

2.4. Texnologiyalarning adolatsiz foydalanishi

Axborot xavfsizligi texnologiyalari, masalan, shifrlash va monitoring vositalari, ko‘pincha adolatsiz foydalanishga olib keladi. Maxfiylikni ta'minlashda ishlatilayotgan texnologiyalar ba'zan hukumatlar yoki tashkilotlar tomonidan fuqarolarning shaxsiy hayotiga aralashish uchun ishlatiladi. Raqamli kuzatuvlar va davlatning internetda foydalanishlarni monitoring qilish amaliyotlari ko‘plab etik savollarni keltirib chiqaradi.

Shuningdek, axborot xavfsizligi texnologiyalarining ba'zi holatlarda korporativ yoki hukumat manfaatlari uchun ishlatilishi, adolatsiz va nohaq raqobatga olib kelishi mumkin. Bu, ayniqsa, internetda hukumatning cheklanmagan nazoratini yaratishda yuzaga keladi.

3. Etik masalalarni hal qilish yo‘llari

3.1. Xususiylik va ma'lumotlarni himoya qilish prensiplari

Axborot xavfsizligida etik masalalarni hal qilish uchun xususiylikni ta'minlash zarur. Foydalanuvchilarga o‘z ma'lumotlarini qanday yig‘ish va ishlatish haqida aniq va oshkora ma'lumot berish, ular bilan o‘rnatilgan shartnomalarni yangilash, va ma'lumotlarni yig‘ishning maqsadini belgilash – axborot xavfsizligini va etikasini ta'minlash uchun muhim qadamlar hisoblanadi.

Foydalanuvchilarga o‘z shaxsiy ma'lumotlarini qanday himoya qilishni o‘rgatish, ularni xavfsiz parollar yaratish, shifrlash va autentifikatsiya usullarini qo‘llashga undash kerak. Bu, etik jihatdan, har bir foydalanuvchining xavfsizlikka oid mas'uliyatini oshiradi.

3.2. Axborot xavfsizligi standartlari va tizimlarining ishlatilishi

Axborot xavfsizligi bo‘yicha xalqaro standartlarni va metodologiyalarni qo‘llash – etik muammolarni hal qilishda muhim vositadir. Bu tizimlar, axborot xavfsizligini ta'minlash va maxfiylikni hurmat qilishni ta'minlashda yordam beradi. Shifrlash usullari, autentifikatsiya protokollari, va axborot tizimlarining muntazam tekshiruvi kabilar, axborot xavfsizligini ta'minlashning mustahkam asoslarini yaratadi.

3.3. Etik kodekslar va ta'lim

Axborot xavfsizligi mutaxassislari uchun etika kodekslarini ishlab chiqish va ularni amalda qo‘llash muhimdir. Kodekslar, axborot xavfsizligi mutaxassislarining ma'lumotlarni to‘plash, saqlash va ulardan foydalanishdagi axloqiy mas'uliyatlarini belgilaydi. Shuningdek,

ta'lim va o‘quv dasturlarini joriy etish, xususiylik va xavfsizlikni ta'minlashda axloqiy xatarlardan saqlanishga yordam beradi.

3.4. Shaxsiy ma'lumotlarga qarshi qonunlar va reglamentlar

Axborot xavfsizligi va etik masalalarni hal qilishda, foydalanuvchilarning huquqlarini himoya qilish uchun qonunchilik va reglamentlarni kuchaytirish zarur. Shaxsiy ma'lumotlarni himoya qilish bo‘yicha yangi qonunlar, masalan, Evropa Ittifoqining GDPR (General Data Protection Regulation) kabi tartibga soluvchi normativ hujjatlar, bu masalalarni hal qilishda katta ahamiyatga ega.

4. Xulosa

Axborot xavfsizligi va etik masalalar o‘rtasidagi bog‘liqlik, raqamli dunyoda faoliyat yuritayotgan barcha sub'ektlar uchun muhim ahamiyatga ega. Shaxsiy xususiylikni himoya qilish, axborotlarni adolatli va ehtiyotkorlik bilan qayta ishlash va texnologiyalarni etik tarzda qo‘llash – bu sohaga oid asosiy vazifalardir. Keng ko‘lamli axborot xavfsizligi muammolarini hal qilish uchun xalqaro hamkorlik, yangilangan qonunlar, ta'lim va yengilliklar kerak. Etik jihatdan to‘g‘ri va xavfsiz raqamli muhit yaratish uchun har bir tomonning mas'uliyati juda katta.

Foydalanilgan adabiyotlar:

1. Anderson, R. (2020). "Security Engineering: A Guide to Building Dependable Distributed Systems." *Wiley*.
2. Solove, D. J. (2008). "The Digital Person: Technology and Privacy in the Information Age." *New York University Press*.
3. Harris, S. (2017). *CISSP All-in-One Exam Guide* (8th ed.). *McGraw-Hill Education*.
4. Vacca, J. R. (2014). *Computer and Information Security Handbook* (3rd ed.). *Elsevier*.
5. Binns, R. (2018). "Ethical Data Use in the Age of Surveillance." *Information Systems Journal*, 28(4), 1-20.