AXBOROT XAVFSIZLIGI VA UNING TA’MINLASH MASALALARI

Sultanbaeva Abadan Temirbaevna-
Muxammed al-Xorezmiy nomidagi Toshkent axborot texnologiyalari universiteti
Nukus filiali 3-kurs talabasi

Annotatsiya

Maqolada axborot xavfsizligi masalasi atroflicha tahlil qilingan va uning davlat, jamiyat hayotiga tasiri, oqibatlari haqida so‘z etilgan.

Kalit so`zlar: Xavfsizlik. Axborot. Axborot xavfsizligi. Axborot texnologiyalari. Kiberxavfsizlik va uning turlari

XXI asr bugungi kunda axborot texnologiyalari va globallashuv asri sifatida baholanmoqda. Zamon shiddat bilan rivojlanayotgan ushbu davrda insonlarning shaxsiy ma`lumotlari, davlat muhim sirlariga oid ma`lumotlarni saqlash muhim hisoblanadi. Ushbu muammo esa axborot xavfsizligi sohasida faoliyat yuritadigan xodimlar uchun katta ma’suliyat yuklaydi.

Axborot xavfsizligi odatda ma'lumotlarning uch jihatini himoya qilish bilan bog‘liq: uning maxfiyligi, yaxlitligi va mavjudligi. Axloq, asosan, huquqlar, zararlar va manfaatlar bilan bog‘liq kompyuter xavfsizligi va huquqlar, zararlar va manfaatlar o‘rtasidagi munosabatlarni o‘rganib chiqib, kompyuter xavfsizligi qanday ma'naviy jihatdan muhim foyda keltirishi mumkin degan

muammo vujudga keladi [1]. Kompyuter xavfsizligi buzilishi natijasida yuzaga kelishi mumkin bo‘lgan birinchi, ehtimol, eng aniq zarar bu iqtisodiy yo‘qotishdir. Tizim xavfsizligi buzilganda, qimmatli apparat va dasturiy ta'minot shikastlangan yoki buzilgan bo‘lishi mumkin va xizmatlar mavjud bo‘lmasligi mumkin, bu esa vaqt, pul va resurslarni behuda sarflashga olib keladi. Axborot xavfsizligini buzish yanada yuqori iqtisodiy xarajatlarga olib kelishi mumkin. Qimmatbaho ma'lumotlar yo‘qolishi yoki zararlanishi mumkin, ular saqlanadigan uskunadan ancha qimmatga tushadi va bu jiddiy iqtisodiy yo‘qotishlarga olib kelishi mumkin ma'lumotlar shikastlanganda yoki yo‘qolganda yo‘qoladi.Har qanday turdagi tizim yoki ma'lumotlar xavfsizligini yo‘qotish ma'lum darajada psixologik yoki hissiy zararga olib kelishi mumkin. Kompyuter xavfsizligini buzish hatto jiddiy zararga olib kelishi mumkin. Masalan, yadroviy reaktorlarni boshqarish, havo harakati va havo harakatini boshqarish, raketa tizimlari va boshqa turdagi tizimlarning buzilishi hayot uchun xavfli oqibatlarga olib kelishi mumkin. Bularga ko‘priklarni loyihalash yoki tibbiy tashxis qo‘yish uchun foydalaniladigan tizimlar qo‘shimcha zarar va huquqlarning buzilishiga olib kelishi mumkin. Tomonlar ma'lumotlarga kirish, nusxa ko‘chirish va tarqatish orqali ma'lumotlarning maxfiyligini xavf ostiga qo‘yishi mumkin. Bunday harakatlar birinchi navbatda mulkiy huquqlarni, shu jumladan, badiiy yoki adabiy asarlar va sanoat namunalari kabi intellektual ijodga egalik qilish va ulardan foydalanish huquqlari bo‘lgan intellektual mulk huquqlarini buzishi mumkin [2] ushbu ma'lumotlarga kirishi va undan foydalanishi mumkin va bu huquq buzilishi mumkin.

Ikkinchidan, konfidensiallikning buzilishi maxfiylik huquqlarini buzishi mumkin.

Mulk huquqlari va shaxsiy hayotning daxlsizligini buzish bilan bir qatorda, maxfiylikni buzish maxfiy ma'lumotlarni tarqatish va ulardan foydalanish natijasida kelib chiqadigan turli xil zararlarni ham keltirib chiqarishi mumkin.

Misol uchun, firmaning ichki eslatmalarini tarqatish uning obro‘siga putur etkazadi va onlayn kredit kartalari bo‘yicha operatsiyalarning maxfiyligini buzish onlayn tranzaktsiyalar xavfsizligiga ishonchni pasaytiradi va elektron bank va elektron tijorat faoliyatiga zarar etkazadi.

Axborotning mavjudligi bo‘yicha murosalar, kengaytirilgan yoki ataylab erkinlik huquqlarini, xususan, axborot erkinligi va so‘z erkinligi huquqlarini buzishi mumkin.

Jeroenvanden Xovenning ta'kidlashicha, axborotga kirish axborot asrida fuqarolarning ma'naviy huquqiga aylandi, chunki axborot asosiy ijtimoiy ne'matga aylandi: jamiyatdagi odamlar muvaffaqiyati uchun zarur bo‘lgan asosiy resurs [3].

Hayotiy axborot xizmatlarining uzilishi axborot olish huquqini buzishi mumkin. Bundan tashqari, kompyuter tarmoqlari xabarlarni tarqatish va boshqalar bilan muloqot qilish uchun veb-saytlar, elektron pochta, xabarlar taxtasi va boshqa xizmatlardan keng foydalaniladi. Bunday xizmatlarga kirish, masalan, xizmat ko‘rsatishni rad etish hujumlari yoki veb-saytlarni o‘g‘irlash orqali bloklanganda, bunday harakatlar so‘z erkinligini buzish sifatida tasniflanadi, odatda, kompyuter xavfsizligi choralari zararni oldini oladi va huquqlarni himoya qiladi, lekin ayni paytda zarar etkazishi va huquqlarni buzishi mumkin.

Shunisi e'tiborga loyiqki, xavfsizlikni boshqarish vositalari axborot va tizim resurslarini shu qadar himoya qilishi mumkinki, ular manfaatdor shaxslarning axborot yoki xizmatlarga kirishiga yo‘l qo‘ymaydi yoki ularni taqiqlaydi: ular foydalanuvchilarning ayrim toifalarini tizimdan foydalanishdan noto‘g‘ri chiqarib tashlashi va foydalanuvchilarning ayrim toifalarini boshqalardan ustun qo‘yishi mumkin.

Kompyuter xavfsizligi sohasida 2001 yil 11 sentyabrdagi hujumlar katta ta'sir ko‘rsatdi. Ushbu xurujlarga javoban milliy xavfsizlik G‘arb davlatlarida asosiy siyosiy muammoga aylandi, bu milliy davlat va uning institutlarining yaxlitligini va uni tahdidlardan, ayniqsa, tashqi tahdidlardan himoya qilish choralarini ko‘rish orqali saqlab qolishdir. 11-sentabr voqealaridan so‘ng G‘arb mamlakatlarida milliy xavfsizlikni himoya qiluvchi ko‘plab yangi qonunlar, qoidalar va dasturlar paydo bo‘ldi, jumladan, butun AQSh Ichki xavfsizlik departamenti tashkil etildi. Bu tashabbuslarning asosiy ahamiyati davlat manfaatlarini terroristik xurujlardan himoya qilishga qaratilgan [4].

Axborot texnologiyalari milliy xavfsizlikni ta'minlashda ikki tomonlama rol o‘ynadi. Avvalo, kompyuter xavfsizligi, ayniqsa, muhim axborot infratuzilmasini tashqi tahdidlardan himoya qilish asosiy ustuvor vazifalardan biriga aylandi. Hukumat kompyuterlari va boshqa davlat va xususiy infratuzilma, shu jumladan Internet va telefon tarmog‘i xavfsizlikni kuchaytirish choralari ko‘riladi.[5]

Ikkinchidan, hukumatlar davlat va xususiy axborot infratuzilmasi ustidan ko‘proq nazorat o‘rnatishga harakat qilishadi. Ular buni ma'lumotlarni tinglash va ushlash, Internet-provayderlar va telefon kompaniyalaridan telefon va elektron pochta yozuvlarini saqlashni va ularni huquqni muhofaza qilish organlari xodimlariga taqdim etishni talab qilish, shifrlashning ayrim shakllarini taqiqlashga urinish yoki hatto kompaniyalardan Internetni teskari muhandislik qilishni talab qilishga urinish orqali qildi. Ajablanarlisi shundaki, hukumatlarning axborot ustidan nazoratni kuchaytirishga qaratilgan bu harakatlari ham xavfsizlikning ma'lum shakllarini kamaytiradi: milliy xavfsizlik bilan bog‘liq hozirgi tashvishlar yangi sabablarga bog`liq holda faylasuf Xelen Nissenbaumning ta'kidlashicha, ular kompyuterlarni davlat idoralari kirishidan kamroq himoya qiladi deb ta'kidlaydi.

Klassik yoki an'anaviy kompyuter xavfsizligi tushunchasi texnik hamjamiyat tomonidan qo‘llaniladigan narsa bo‘lib, kompyuter xavfsizligini ma'lumotlarning xavfsizligi va yaxlitligi, mavjudligi va maxfiyligi nuqtai nazaridan belgilaydi.

U kiberxavfsizlik deb ataydigan ikkinchisi, axborot infratuzilmasini milliy manfaatlarga tahdidlardan himoya qilish bilan shug‘ullanadi. Biroq, kiberxavfsizlikning asosi milliy xavfsizlik va ayniqsa, davlatning terroristik hujumlarga zaifligi bilan bog‘liq xavotirlardir. [6]

Texnik kompyuter xavfsizligi jismoniy shaxslar va tashkilotlarning, xususan, kompyuter tizimlari va ma'lumotlarining egalari va foydalanuvchilarining shaxsiy manfaatlarini himoya qilishga qaratilgan.

Kiberxavfsizlik milliy davlat manfaatlarini himoya qilishga qaratilgan va kompyuter xavfsizligini milliy xavfsizlikning tarkibiy qismi sifatida ko‘rib chiqadi. Texnik kompyuter xavfsizligi choralari asosan kompyuter tizimlarini tashqi hujumlardan himoya qiladi [7].

Kiberxavfsizlik tashabbuslari, shuningdek, bunday himoya choralarini o‘z ichiga oladi, lekin ular qarshi choralarni tavsiya qilganda, ikkita xavfsizlik tushunchasi bir-biriga zid keladi.

Masalan, kiberxavfsizlik kompyuter tizimini masofaviy hukumat tekshiruvi uchun ochishni talab qilishi yoki hukumatdan veb-saytlarga ularni yopish uchun kirishni talab qilishi mumkin, texnik kompyuter xavfsizligi esa bunday harakatlarni taqiqlashi mumkin.

Texnik kompyuter xavfsizligi va kiberxavfsizlikning turli xil manfaatlari ma'naviy ikkilanishlarni keltirib chiqarishi mumkin: davlat manfaatlari yoki xususiy tomonlarning manfaatlari va huquqlari ustuvor bo‘lishi kerakmi, bu milliy xavfsizlik manfaatlarini fuqarolik huquqlari bilan qanday muvozanatlash kerakligi haqidagi katta dilemmaga ishora qiladi [1].

Kompyuter xavfsizligining ko‘p qismi kompyuter resurslari va ma'lumotlarini ruxsatsiz, qasddan buzish yoki nosozlikdan himoya qilish bilan bog‘liq hisoblanadi.

Xakerlar yuqori malakali kompyuter foydalanuvchilari bo‘lib, ular o‘zlarining iste'dodlaridan bunday kirish uchun foydalanadilar va ko‘pincha bilim va ma'lumotlarni almashish uchun boshqa xakerlar bilan jamoalar yoki tarmoqlar tashkil qiladilar. Buzg‘unchilik ko‘pincha zararli maqsadlarda bunday ruxsatsiz kirishni qo‘lga kiritish sifatida ham ta'riflanadi: ma'lumot va dasturiy ta'minotni o‘g‘irlash yoki ma'lumotlarni buzish yoki tizim ishini buzish.

Biroq, o‘z-o‘zini identifikatsiya qilgan xakerlar xakerlik deb ta'riflagan noma'lum buzg‘unchilar bilan xakerlik deb ataydigan zararli va buzg‘unchi xakerlar o‘rtasida farq qiladilar [3] zarar keltiradi va buning o‘rniga ijobiy ta'sir ko‘rsatadi.

Ularning fikriga ko‘ra, xakerlik faoliyatining ijobiy ta'siri shundaki, u barchaning manfaati uchun ma'lumotlarni ozod qiladi, shuningdek, xavfsizlik teshiklarini ochib, tizimlar va dasturiy ta'minotni yaxshilaydi [3], bu ko‘plab xakerlarning faoliyatini boshqaradigan (odatda yashirin) tamoyillar to‘plami hisoblanadi. Kompyuterlarga kirish cheklanmagan va to‘liq bo‘lishi uchun va kiberfazoda faoliyat real dunyoda zarar keltirmasligi uchun bepul bo‘lishi kerak, xakerlik etikasining ko‘plab tamoyillarini qo‘llab-quvvatlab bo‘lmaydi deb ta'kidladi Xerman Tavani [3].

Axborotning erkin bo‘lishi kerakligi haqidagi e'tiqod intellektual mulk tushunchasiga zid bo‘lib, axborotni yaratuvchilar uni saqlashga yoki undan foyda olishga haqli emasligini anglatadi, shuningdek, bu shaxsiy daxlsizlikni tubdan buzadi va uning yaxlitligi va aniqligiga putur etkazadi.

Herman Tavani, shuningdek, xavfsizlik kamchiliklarini ko‘rsatishda xakerlik foydasi u keltiradigan zarardan ustun bo‘lolmasligini va kibermakondagi faoliyat real dunyoda zarar keltirishi mumkinligini ta'kidlaydi. Buzg‘unchilik ham, xakerlik ham odatda noqonuniydir va shuning uchun kompyuter jinoyati yoki kiberjinoyatning bir turi sifatida tasniflanishi mumkin [2,4].

Kompyuter xavfsizligiga tahdid soladigan kiberjinoyatlarning ikkita asosiy turi mavjud: kiberjinoyat va kiber vandalizm. Kompyuter tarmoqlarini buzadigan yoki ma'lumotlarni buzadigan dasturlarni ochish uchun axborot texnologiyalaridan foydalanadigan, ba'zan kompyuter xavfsizligini buzish, kiber jinoyatlarni o‘z ichiga olgan uchinchi turdagi kiber jinoyatlar ajralib turadi.

Kiberqaroqchilik, shuningdek, dasturiy ta'minot qaroqchiligi deb ataladi, bu xususiy dasturiy ta'minot yoki ma'lumotlarning nusxalarini ko‘paytirish yoki bunday ma'lumotlarni kompyuter tarmog‘ida tarqatish uchun axborot texnologiyalaridan foydalanish hisoblanadi.

Kiberqaroqchilik kibervandalizm yoki kiberjinoyatga qaraganda ancha keng tarqalgan. Chunki u keng ko‘lamli kompyuter ko‘nikmalarini talab qilmaydi va ko‘plab kompyuter foydalanuvchilari mualliflik huquqi bilan himoyalangan dasturiy ta'minot va ma'lumotlarning nusxalarini yaratishni axloqiy jihatdan maqbul deb bilishadi.

Kiberjinoyat mualliflik huquqini himoya qilishni buzish bilan bog‘liq bo‘lib, kompyuter xavfsizligini buzishni o‘z ichiga oladi. ba'zan kompyuter xavfsizligini buzishni o‘z ichiga oladi, bu kompyuter firibgarligi bo‘lib, Internetda yolg‘on identifikatsiya qilish yoki o‘zgartirish orqali onlayn biznes operatsiyalarida shaxsiy manfaatlar uchun aldashdir yoki ma'lumotlarni buzish

Kompyuter firibgarligi parollar, raqamli identifikatorlar yoki boshqa tranzaksiya yoki kirish kodlarini olish uchun kiberjinoyatchilik faoliyatini, shuningdek, parollarni o‘zgartirish bilan bog‘liq kibervandalizmni o‘z ichiga olishi mumkin ma'lumotlar hisoblanadi.

So‘nggi paytlarda kompyuter va milliy xavfsizlik masalasi kiberterrorizm ehtimoli bilan bog‘liq bo‘lib, Herman Tavanik tomonidan "jiddiy zarar etkazishga qaratilgan, ya'ni odamlarning halok bo‘lishiga yoki jiddiy iqtisodiy yo‘qotishlarga olib keladigan siyosiy sabablarga ko‘ra xakerlik operatsiyalari" deb ta'riflanadi [3].

Ushbu infratuzilmani zaiflashtirish yoki buzish va unga bog‘liq bo‘lgan iqtisodiy, sanoat yoki ijtimoiy tuzilmalarga zarar yetkazishni maqsad qilgan axborot infratuzilmasiga yirik hujumlar ehtimoli bugungi kunda katta tashvishga aylandi.

O‘z ishining ma'naviy jihatini baholash va unda axloqiy dilemmalar bilan shug‘ullanish uchun ular axborot xavfsizligi axloqi bo‘yicha treningni talab qiladilar. va ularning faoliyatidagi dilemmalar va bunday axloqiy muammolarni hal qilishda turli axloqiy tamoyillarni muvozanatlashtiradi [1,2].

Foydalanilgan adabiyotlar:

1.Буряк Н.Ю Лингвопедагогическая культура. Учебное пособие для студентов направления подготовки бакалавриата (учебное пособие) Краснодар: Издательский дом «ХОРС», 2013.- 404с

2.Буряк Н.Ю. Язык - культура — ментальность (научная статья). Сборник научных трудов по материалам конференции «Интеграция науки и практики как механизм эффективного развития современного общества» (г. Москва,3- 4июля 2014г.) - Москва,2014.-С.262-269.

3.Tavani,H.:.Ethicsand Technology: Ethical Issuesinan Age of information and Communication Technology (Wiley, 2014)

4.Bullock, J., et al.: Introduction to Homeland Security, 1st edn (ButterworthHeinemann, 2015)

5.Seitnazarov K.K. Integration of gis technology for fuzzy deterministic simulation of conditions of operation and maintenance Kegeyli groundwater is abstracted// «IJRET» Volum 4 Issue 2. – Indiya, 2015. – P.727-735. eISSN: 2319-1163/pISSN: 2321-7308.

6. Усманов Р.Н., Сеитназаров К.К. Об организации параллельных вычислений в процессе решения геофильтрационных задач // Вестник ТУИТ. – Ташкент, 2014. - № 1. – С. 101-106. ISSN 2010-9857

7. К.К. Сеитназаров, Н.С. Мухиятдинов, М.М. Урынбаева. Искусственный интеллект и его применение в принятии решений: методы, алгоритмы и перспективы// Journal of Universal Science Research, 2023.