AXBOROT TIZIMLARIGA EXTIMOLIY XUJUMLARNI BAXOLASH VA MATEMATIK KUTILMASINI MODELLASHTIRISH

Samandarov Batirbek Satimovich[1,2], Tajibaev Shuxrat Xudaybergenovich[3]

[1] *Muhammad al-Xorazmiy nomidagi Toshkent Axborot Texnologiyalari Universiteti*
[2] *Soliq qo'mitasi huzuridagi Fiskal insituti*
[3] *Berdaq nomidagi Qoraqalpoq davlat universiteti*
[1,2] *PhD, dotsent. e-mail: batirbeksamandarov@gmail.com*
[3] *katta o'qituvchi. e-mail: tajibaevsx@gmail.com*

KALIT SO'ZLAR

axborot tizimi, axborotni ximoyalash, xavfsizlikka tahdidlar, himoya usullari, axborot tizimiga xujumning matematik kutilmasi.

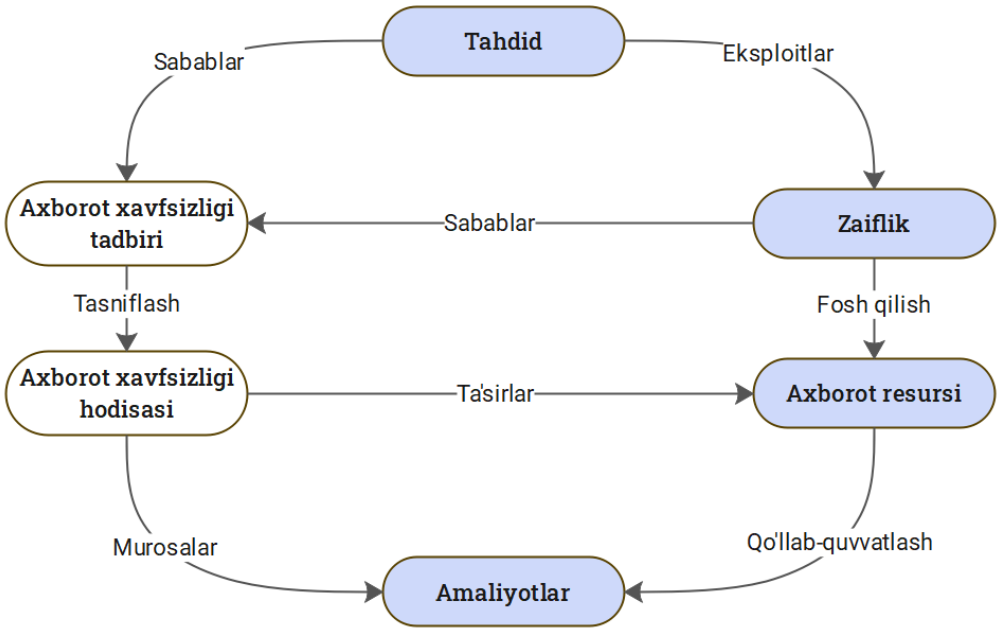
ANNOTATSIYA

Ushbu maqolada axborot tizimlariga extimoliy hujumlarni baholash masalasi, axborot tizimlarining kutilmagan holatlar sababli ishlamay qolishining matematik kutilmasi darajasiga va ularning murakkabligiga ko'ra tasniflab chiqilgan. Shuningdek, axborot tizimining ishonchliligini baholash va ma'lum bir vaqt oralig'ida kutilishi mumkin bo'lgan o'rtacha nosozliklarni aniqlash uchun axborot tizimining ishdan chiqishi matematik kutilmasi modellashtirilgan. Ushbu modelga tayangan holda, ayrim cheklangan parametrlarga asoslangan axborot tizimiga xujum qilinish extimolligi baholangan.

I. Kirish

Bugungi axborotlashgan jamiyatda iqtisodiyotimizning turli xil sohalari uchun ishlab chiqilayotgan va joriy qilinayotgan zamonaviy axborot tizimlari hayotimizda muhim o'rin tutadi, bizga turli xizmatlardan foydalanish imkoniyatini beradi va muhim shaxsiy ma'lumotlarni saqlash imkoniyatini yaratadi[1,2].

Axborot xavfsizligi hodisasidagi ob'ektlarning o'zaro bog'lanishi axborot tizimining turli elementlari yoki komponentlari hodisa yoki xavfsizlik buzilishi sharoitida bir-biri bilan bog'liq bo'lishi mumkinligini anglatadi. Ushbu ob'ektlar texnik yoki texnik bo'lmagan bo'lishi mumkin va ularning o'zaro ta'siri hodisaning sababi yoki natijasi bo'lishi mumkin.



1-rasm. Axborot xavfsizligi hodisasida ob'ektlarning o'zaro munosabati

Oxir oqibat, axborot tizimlarining xavfsizligini ta'minlash kompleks yondashuvni, shu jumladan tahdidlarni baholashni, tegishli xavfsizlik choralarini qo'llashni, tizimni doimiy ravishda yangilab turishni va monitoringini talab qiladi. Bu axborot tizimlarini favqulodda hujumlardan ishonchli himoya qilishni ta'minlash va ma'lumotlarning maxfiyligi va yaxlitligiga tahdidlarning oldini olishning yagona yo'li.

II. TAXLILLAR

Tadqiqotlar shuni ko'rasatadiki, har qanday axborot tizimlarining potentsial afzalliklariga qaramasdan, ularni joriy qilishda o'ziga xos murakkabliklar kelib chiqadi[3]. Axborot texnologiyalaridan foydalanish ortib borayotgani sari, maxfiy ma'lumotlarga turli xil usullar yordamida buzib kirishga urinishlar[4], korxona va tashkilotlar ma'lumotlariga xujumlar eng xavfli tahdidlardan biri bo'lib bormoqda[5,6].

IBM tadqiqotlariga ko'ra, ma'lumotlar buzilishining o'rtacha narxi 2023-yilda 4,45 million dollarni tashkil qilib, tarixdagi eng yuqori ko'rsatkichga etgan. O'rganish natijalariga ko'ra bu 2022 yildagi 4,35 million dollarlik xarajatlarga nisbatan 2,3 foizga oshgani aniqlandi. Uzoq muddatli o'rtacha xarajat 2020 yil hisobotida qayd etilgan 3,86 million dollardan 15,3 foizga oshgan [7].

Bugungi kunda axborot tizimlarini ishlab chiqish va ularning xavfsiligini ta'minlash bo'yicha ishlab chiqilayotgan me'yoriy xujjatlar [8,9,10,11,12,13] axborot tizimlarining o'sib borayotgan murakkabliklarini hisobga olmasdan ishlab chiqilgan, shuningdek bugungi kun talablariga mos ravishda yangilab borilmayapdi.

III. ASOSIY QISM

Murakkab axborot tizimlari va avtomatlashtirilgan tizimlariga ham oddiy tizimlar bilan bir xil darajadagi talablar quyilishi va amalga oshirilishi, oddiy axborot tizimlari va avtomatlashtirilgan tizimlar uchun zarur bo'lgan talablarning oshib ketishiga, o'z navbatida esa murakkab zamonaviy tizimlar uchun bu talablarning etarli emasligiga olib keladi. Zamonaviy axborot tizimlarining murakkablik darajasi oshib borishi bilan axborot tizimlarining xavfsizlik talablarini ularning murakkablik darajasiga ko'ra tasniflashning tabiiy ehtiyoji paydo bo'ldi.

Axborot tizimlarining ishlamay qolish vaqtining matematik kutilmasi va ularning murakkabligi bo'yicha tavsiflanishi.

Axborot tizimlarini va avtomatlashtirilgan tizimlarni kutilmagan holatlar sababli ishlamay qolish vaqtini matematik kutilmasi darajasiga va ularning murakkabligiga qarab tasniflash mumkin. Kutilmagan holatlar sababli ishlamay qolish vaqtini matematik kutilmasini to'rtta darajaga (past, o'rta, yuqori, juda yuqori) va tizimning murakkabligini to'rtta (past, o'rta, yuqori, juda yuqori) darajaga ajratamiz:

Jadval 1. Matematik kutilma past darajada bo'lgan tasniflash

Matematik kutilma darajasi	***Tizim murakkablik darajasi***	***Tizimlarga misollar***
Past	*Past*	*Ishonchliligi past bo'lgan oddiy tizimlar, masalan, kichik uy axborot tizimlari yoki qurilmalarni boshqarish uchun oddiy avtomatlashtirilgan tizimlar*
Past	*O'rta*	*O'rta murakkablik va ishonchlilikdagi tizimlari, masalan, katta bo'lmagan biznes tizimlari yoki mahalliy tarmoqlar*
Past	*Yuqori*	*Murakkabligi yuqori, ammo ishonchliligi past bo'lgan tizimlar, masalan, qiyinchilik bilan ishlaydigan murakkab biznes tizimlari*
Past	*Juda yuqori*	*Ishonchlilik talablari yuqori bo'lgan murakkab tizimlar, masalan, yirik korporativ axborot tizimlari yoki ishlab chiqarishni boshqarish tizimlari*

Jadval 2. Matematik kutilma o‘rta darajada bo‘lgan tasniflash

Matematik kutilma darajasi	***Tizim murakkablik darajasi***	***Tizimlarga misollar***
O‘rta	*Past*	*O‘rtacha murakkablik va past ishonchlilikdagi tizimlar, masalan, kichik tashkilotlar uchun muhim bo‘lmagan axborot tizimlari*
O‘rta	*O‘rta*	*O‘rtacha murakkablik va ishonchlilikdagi tizimlar, masalan, ma’lumotlar bazasini boshqarish tizimlari yoki banklar uchun o‘rta axborot tizimlari*
O‘rta	*Yuqori*	*Yuqori murakkablikdagi, ammo ishonchliligi o‘rtacha bo‘lgan tizimlar, masalan, ishlab chiqarishni cheklangan zahira bilan boshqaruvchi murakkab tizimlar*
O‘rta	*Juda yuqori*	*Ishonchliligi yuqori bo‘lgan murakkab tizimlar, masalan, havo harakatini boshqarish tizimlari yoki elektr energiyasini taqsimlash tizimlari*

Jadval 3. Matematik kutilma yuqori darajada bo‘lgan tasniflash

Matematik kutilma darajasi	***Tizim murakkablik darajasi***	***Tizimlarga misollar***
Yuqori	*Past*	*Ishonchliligi yuqori, ammo murakkabligi past tizimlar, masalan, kirishni boshqarish tizimlari yoki videokuzatuv tizimlari*
Yuqori	*O‘rta*	*O‘rtacha ishonchlilikdagi murakkab tizimlar, masalan, transport oqimini boshqarish tizimlari yoki yirik banklar uchun murakkab axborot tizimlari*
Yuqori	*Yuqori*	*Yuqori murakkablik va ishonchlilikka ega bo‘lgan murakkab tizimlar, masalan, energetika ob’ektlari uchun murakkab boshqaruv tizimlari yoki davlat boshqaruv idoralari uchun katta axborot tizimlari*
Yuqori	*Juda yuqori*	*Juda yuqori ishonchlilik va murakkablikka ega bo‘lgan muhim tizimlar, masalan, atom elektr stantsiyalarini yoki aviatsiya parvozlarini boshqarish tizimlari*

Jadval 4. Matematik kutilma juda yuqori darajada bo‘lgan tasniflash

Matematik kutilma darajasi	***Tizim murakkablik darajasi***	***Tizimlarga misollar***
Juda yuqori	*Past*	*Ishonchlilik darajasi juda yuqori, ammo murakkabligi past bo‘lgan murakkab tizimlar, masalan, tibbiy asboblarni boshqarish tizimlari*
Juda yuqori	*O‘rta*	*Juda yuqori ishonchlilik va o‘rtacha murakkablik darajasidagi murakkab tizimlar, masalan, omborlarni avtomatik boshqarish tizimlari yoki yirik tibbiyot muassasalari uchun murakkab axborot tizimlari*
Juda yuqori	*Yuqori*	*Yuqori murakkablik va juda yuqori ishonchlilikka ega bo‘lgan muhim tizimlar, masalan, kosmik parvozlarni boshqarish tizimlari yoki yirik moliya institutlari uchun murakkab axborot tizimlari*
Juda yuqori	*Juda yuqori*	*Ishonchliligi va murakkabligi juda yuqori bo‘lgan murakkab tizimlar, masalan, qurolli kuchlarni boshqarish tizimlari yoki yirik global kompaniyalar uchun yirik axborot tizimlari*

Axborot tizimlarining xujumlar tufayli ishdan chiqishining matematik kutilmasini modellashtirish

Axborot tizimlarining ishdan chiqishining matematik kutilmasi - bu tizimning ishonchliligini baholash uchun ishlatiladigan va ma’lum vaqt ichida kutilishi mumkin bo‘lgan o‘rtacha nosozliklar sonini ifodalovchi ko‘rsatkich

sanaladi. Bu orqali kelib chiqishi mumkin bo‘lgan nosozliklar ehtimolini taxmin qilish va tizimning ishonchliligini oshirish choralarini ko‘rish zarurligini baholash imkonini beradi.

Axborot tizimlarining ishdan chiqishining matematik kutilmasini quyidagicha hisoblaymiz:

$$E(T) = \sum(n * P(n))$$

Bu erda:

$E(T)$ – ishdan chiqishning matematik kutilmasi;

n – ishdan chiqishlar soni;

$P(n)$ – nosozlikning n marta sodir bo‘lish extimolligi;

Ushbu model yordamida xujumlar natijasida axborot tizimi ishdan chiqishini oldindan baholab borish, axborot tizimini ximoya qilish chora-tadbirlari samaradorligini baholash, ximoya chora-tadbirlariga ustuvorlik berish va tizimni xujumdan keyin tez tiklashga erishishni ta’minlab beradi.

Axborot tizimiga hujumlarni baholash

Ehtimollar nazariyasi yordamida axborot tizimiga hujumlarni baholash turli usullar va modellar yordamida amalga oshirilishi mumkin. Bu erda qo‘llanilishi mumkin bo‘lgan bir nechta yondashuvlar mavjud:

1. **Tahdid modeli:** har xil turdagi hujumlar va ularning ehtimolliklarini tavsiflovchi model qurish orqali. Buni avvalgi hujumlar statistikasi yoki ekspert baholari asosida amalga oshirish mumkin. Masalan, veb-dastur yoki ijtimoiy muhandislikdagi zaifliklar orqali hujum ehtimoligi aniqlanadi.
2. **Zaifliklar tahlili:** axborot tizimidagi zaifliklar asosida muvaffaqiyatli hujum ehtimolini baxolab olamiz. Bu tizim arxitekturasidagi zaif tomonlarni, har xil turdagi hujumlardan himoya darajasini va ularning mumkin bo‘lgan oqibatlarini tahlil qilishni o‘z ichiga oladi. Bunda, ba’zi zaifliklardan foydalanish ehtimoli yuqori, boshqalari esa kamroq bo‘lishi mumkinligi hisobga olinadi.
3. **Xatarlar tahlili:** hujumning mumkin bo‘lgan oqibatlarini va ularning ehtimolligi baholanadi. Bu orqali axborot tizimiga eng muhim tahdidlarni aniqlashga erishiladi. Masalan, mijozlarning nozik ma’lumotlarini sizdirilishiga olib kelishi mumkin bo‘lgan hujum, xizmatni vaqtincha rad etishga olib keladigan hujumdan ko‘ra jiddiyroq oqibatlarga olib kelishi mumkin.
4. **Ehtimollik modellarni ishlab chiqish:** tahdidlar turlari, tizimlar turlari va xavfsizlik choralari kabi turli omillarga asoslangan hujum ehtimolini bashorat qila oladigan ehtimoliy modellarni ishlab chiqish uchun statistik ma’lumotlardan foydalanish mumkin. Masalan, katta hajmdagi ma’lumotlarni tahlil qilish va oldin kuzatilgan xujum taxlillari asosida hujumlar ehtimolini taxmin qilish uchun mashinali o‘qitish modellaridan foydalanish mumkin bo‘ladi.

Shuni ta’kidlash kerakki, axborot tizimiga hujum uyushtirilishi ehtimolini baholash qiyin vazifa bo‘lib, odatda natijalar taxminiy bo‘lishi mumkin. Shu bilan birga, ehtimollar nazariyasi va xavflarni tahlil qilishdan foydalanish eng muhim tahdidlarni aniqlashga va axborot tizimining xavfsizligini ta’minlash uchun oldindan tegishli choralarni ko‘rib qo‘yishga yordam beradi.

Axborot tizimiga xujumlar extimolligini baholash

Hujum ehtimoliga ta’sir qiluvchi ko‘plab faktorlar tufayli ehtimollik nazariyasiga ko‘ra axborot tizimiga hujumlarni baholash uchun aniq matematik formulani shakllantirish murakkabliklar keltirib chiqarishi mumkin. Ayrim parametrlarni hisobga olgan holda, cheklangan parametrlarga asoslangan hujum ehtimoligini baholash uchun quyidagicha belgilashlar kiritib olamiz:

$P(A)$ – axborot tizimiga hujum qilish ehtimolligi;

$P(V)$ – axborot tizimida zaifliklar mavjudligi ehtimolligi;

$P(E)$ – axborot tizimidagi mavjud zaiflikdan muvaffaqiyatli foydalanilish ehtimolligi;

$P(M)$ – g‘araz niyatli shaxsni axborot tizimiga xujum uyushtirishga undalishi ehtimolligi;

Ushbu holatda axborot tizimiga xujum qilishinish ehtimolligini quyidagi formula asosida baholash mumkin bo‘ladi:

$$P(A) = P(V) * P(E) * P(M)$$

Ushbu formulada hujum ehtimolligi tizimdagi zaiflik ehtimolliligiga ($P(V)$), axborot tizimidagi mavjud zaiflikdan muvaffaqiyatli foydalanilish ehtimolligi ($P(E)$) va g‘araz niyatli shaxsni axborot tizimiga xujum uyushtirishga undalishi ehtimolliklariga ($P(M)$) bog‘liq deb taxmin qilinadi.

Biroq, aslida, hujum ehtimoli ko‘plab boshqa omillarga bog‘liq bo‘lishi mumkin, masalan, hujumlar turlari, xavfsizlik choralari, tizimning murakkabligi va boshqalar. Shu sababli, hujum ehtimolini aniqroq va murakkab baholash yanada murakkab modellarni ishlab chiqishni yoki ko‘proq statistik ma‘lumotlarga tayanishni talab qilishi mumkin.

Axborot tizimiga hujumlar ehtimolini baholash axborot xavfsizligini boshqarishning muhim vositasi hisoblanadi. Yuqoridagilardan kelib chiqilsa, axborot tizimiga bo‘ladigan xujumlarni oldindan baholab borish axborot tizimi himoyasi bo‘yicha ongli qarorlar qabul qilish va hujumlar xavfini kamaytirish imkonini beradi.

IV. Xulosa

Xulosa qilib aytadigan bo‘lsak, axborot tizimlariga favqulodda hujumlarni baholash va xavfsizlik choralarini ta’minlash bugungi raqamli dunyoda muhim jihatlardir. Tahdidlarni to‘g‘ri baholash va tegishli xavfsizlik choralarini ko‘rish axborot tizimlarini g‘araz niyatli shaxslardan himoya qilish va hujumlarning mumkin bo‘lgan salbiy oqibatlarini minimallashtirish imkonini beradi. Xavfsizlik tizimini doimiy yangilash va takomillashtirish axborot tizimlari xavfsizligini ta’minlashning ajralmas qismi hisoblanadi.

Oxir oqibat, axborot tizimlari xavfsizligini ta’minlash tahdidlarni baholash, tegishli xavfsizlik choralarini qo‘llash, tizimni doimiy yangilash va monitoringini o‘z ichiga olgan kompleks yondashuvni talab qiladi. Faqat shu yo‘l bilan biz axborot tizimlarini favqulodda hujumlardan ishonchli himoya qilishni ta’minlashimiz va ma’lumotlarning maxfiyligi va yaxlitligiga yuzaga kelishi mumkin bo‘lgan tahdidlarning oldini olishimiz mumkin.

V. Adabiyotlar

1. Muminov B. B., Karimov U. U., Bekmurodov U. B. Models of integration of information systems in higher education institutions //2020 IEEE 14th International Conference on Application of Information and Communication Technologies (AICT). – IEEE, 2020. – С. 1-5.
2. Самандаров Б.С., Сарсенбаев К.К., Гулмирзаева Г.А. Олий таълим муассасаларида компьютер техникалари ҳисобини юритишда RFID технологияларидан фойдаланишнинг долзарб жиҳатлари // International Scientific and Technical Conference “Digital Technologies: Problems and Solutions of Practical Implementation in the Industry” –Tashkent-2023, april 27-28, –P. 34-36
3. Самандаров Б.С., Гелдибаев Б.Е., Олламберганов Ф.Ф., Гулмирзаева Г.А. Чорва фермаларининг радиочастотали идентификациялаш тизими инфратузилмасини лойиҳалаш // Digital Transformation and Artificial Intelligence. 1(2), 68–72.
4. Mamatov N.S., Abdukadirov B.A., Samijonov A.N., Samijonov B.N. Method for false attack detection in face identification system // International Conference on Information Science and Communications Technologies: Applications, Trends and Opportunities, ICISCT 2021, 2021
5. Самандаров Б.С., Тажибаев Ш.Х. Web иловалар маълумотлар базаси хавфсизлигини таъминлашда SQL сўровлар заифлигига асосланган тахдидларни бартараф килиш усуллари // «Фан ва жамият» илмий услубий журнал, №2. Нукус-2020. –Б. 10-12
6. Nishanov A.X. Samandarov B.S. SQL so’rovlar zaifligiga asoslangan taxdidlar majmuasini aniqlash usullari va ularni bartaraf qilish bosqichlari // «Matematikaning zamonaviy muammolari» respublika ilmiy onlayn anjumani. Nukus-2020. –B. 244-245

7. IBM. Cost of a Data Breach Report 2023 / [Электрон манба] https://www.ibm.com/reports/data-breach (мурожаат санаси: 10.09.2023).
8. O‘z DSt 1986:2018. Ахборот технологияси. Ахборот тизимлари. Яратиш босқичлари. Ўзбекистон Республикасининг давлат стандарти. Киритиш санаси 2018-14-06. – Т. : Ўзбекистон стандартлаштириш, метрология ва сертификатлаштириш агентлиги, 2018. – 17 б.
9. O‘z DSt 3386:2019 (ISO/IEC 27035-1:2016, MOD). Информационная технология. Методы обеспечения безопасности. Управление инцидентами информационной безопасности. Часть 1. Принципы управления инцидентами. Государственный стандарт Республики Узбекистан. Дата введения 01.04.2019. – Т. : Узбекское агентство стандартизации, метрологии и сертификации, 2019. – 38 с.
10. Standard ISO/IEC 27006:2007. Information technology. Security techniques. Requirements for auditing bodies and certification of information security management systems. 2007. 44 p. Available at: http://www.pqm-online.com/assets/files/lib/std/iso_iec_27006-2007.pdf (accessed 15.09.2023).
11. ISO/IEC FDIS 17799:2005. Information technology – Security techniques.- Code of practice for information security management. ITTF, 2005. 129 p. – Available at: http://comsec.spb.ru/matherials/is/iso17799-2005.pdf (accessed 15.09.2023).
12. ISO/IEC FDIS 27001:2005. Information technology - Security techniques - Information security management systems – Requirements. ISO/IEC, 2005. 42 p. – Available at: http://www.itref.ir/uploads/editor/42890b.pdf (accessed 20.09.2023).
13. ГОСТ Р 57564–2017. Организация и проведение работ по международной стандартизации в Российской Федерации : нац. стандарт Рос. Федерации : дата введения 2017-12-01. – М. : Стандартинформ, 2017. – 43 с.