AXBOROT HUJUMLARI, KOMPYUTER VIRUSLARI VA ULARDAN HIMOYALANISH USULLARI

Kodirova Dilfuzaxon Abrorxonovna
Toshkent "Temurbeklar maktabi" harbiy-akademik litseyi informatika va axborot texnologiyalari fani bosh o'qituvchisi
https://doi.org/10.5281/zenodo.15705157

ARTICLE INFO

Qabul qilindi: 10-Iyun 2025 yil
Ma'qullandi: 14-Iyun 2025 yil
Nashr qilindi: 20-Iyun 2025 yil

KEYWORDS

axborot hujumi, raqamli tahdid, himoya strategiyasi, xavfsizlik protokoli, kiberxavfsizlik, psixologik hujum, ma'lumotlarni himoya qilish

ABSTRACT

Ushbu maqolada raqamli xavfsizlikka tahdid soluvchi zamonaviy axborot hujumlari tahlil qilinadi. Ularni amalga oshirilish usullari, xavf omillari va salbiy ta'siri haqida fikr yuritilib, tajriba va texnologiyalar asosida himoya choralariga baho beriladi. Ayrim fikrlar sun'iy intellekt vositalaridan foydalangan holda tahrirlanib taklif etilgan.

Axborot texnologiyalari jadal sur'atlar bilan hayotimizning ajralmas qismiga aylanar ekan, ular bilan bog'liq xavfsizlik masalalari ham dolzarb tus olmoqda. Axborot resurslariga egalik qilish bugungi raqamli dunyoda strategik ustunlikni belgilaydi. Shu sababli, texnologik infratuzilmalarning murakkabligi va kengayishi bilan birga, ularga qaratilgan tahdidlar soni ham ortmoqda [1, 12-16 b.].

Hozirgi kunda axborot hujumlari turli shakllarda ko'zga tashlanmoqda: texnik ekspluatatsiyalar, ijtimoiy muhandislik vositalari, ichki sabotajlar yoki yolg'on axborot tarqatish orqali amalga oshirilayotgan dezinformatsiya kampaniyalari bunga misoldir. Bularning har biri nafaqat tizimlar barqarorligiga, balki foydalanuvchi ishonchiga, iqtisodiy barqarorlikka va davlat xavfsizligiga ham jiddiy tahdid soladi.

Axborot hujumlarining turlari Axborot hujumlari texnologik va psixologik yondashuvlar asosida amalga oshiriladi. Ular quyidagi asosiy turlarga bo'linadi:

1. **Zararli dasturlar:** Viruslar, troyanlar, josuslik dasturlari (spyware), reklama dasturlari (adware), va shifrlovchi dasturlar (ransomware) orqali tizimga zarar yetkazish yoki foydalanuvchi ustidan nazorat o'rnatish.

2. **Xakerlik hujumlari:** Maxfiy ma'lumotlarga noqonuniy kirish, tarmoq zaifliklarini ekspluatatsiya qilish va xizmatni rad etish hujumlarini o'z ichiga oladi. DDoS hujumlari orqali xizmatlar ishdan chiqariladi. Zero-day ekspluatatsiyalar orqali ilgari noma'lum bo'lgan xatoliklardan foydalaniladi [2, 45-51 b.; 7].

3. **Ijtimoiy muhandislik:** Ijtimoiy muhandislik bu kiberxavfsizlikdagi eng xavfli va ayni paytda eng murakkab hujum turlaridan biridir. Uning asosiy tamoyili texnologik vositalardan ko'ra inson omiliga tayanadi. Bu usulda hujumchilar psixologik, sotsiologik yoki madaniy

jihatlarni o‘rganib, foydalanuvchilarning ishonchiga kirish orqali ulardan muhim ma'lumotlarni (login, parol, bank rekvizitlari) olishga intilishadi [4, 92-96 b.; 6].

Ijtimoiy muhandislik turli shakllarda namoyon bo‘ladi:

- **Phishing (soxta pochta xabarlari):** Hujumchi rasmiy ko‘rinishdagi elektron xat orqali foydalanuvchini maxsus havolaga o‘tishga undaydi. Bu havola orqali foydalanuvchi ma’lumotlarini kiritgan zahoti ular hujumchining qo‘liga tushadi.
- **Spear Phishing:** Maqsadli hujum bo‘lib, bu yerda hujumchi aniq bir shaxs yoki tashkilotni nishonga oladi. Xabar mazmuni foydalanuvchiga moslashtirilgan bo‘ladi, bu esa uning haqiqatga o‘xshash darajasini oshiradi.
- **Pretexting (uydirma sabab bilan ma’lumot so‘rash):** Hujumchi o‘zini tashkilot xodimi, texnik yordamchi yoki tanish sifatida ko‘rsatib, turli bahonalar bilan maxfiy ma’lumotlarni olishga urinishadi.
- **Baiting (qiziqtirish):** Foydalanuvchiga bepul dastur, musiqiy fayl yoki boshqa jozibador kontent taklif qilinadi, aslida esa bu fayl zararli dastur bo‘lib chiqadi.
- **Quishing (QR-code phishing):** QR-kodlar yordamida foydalanuvchilarni zararli veb-saytlarga yo‘naltirish orqali ma’lumot yig‘iladi.
- **Tailgating (yopiq hududga kuzatish):** Bu usulda hujumchi binoga kirish uchun haqiqiy xodim ortidan kiradi, ko‘pincha o‘zini unutuvchan xodim sifatida ko‘rsatadi.

Ijtimoiy muhandislik hujumlari texnik zaiflikdan ko‘ra, insonning e’tiborsizligi, ishonuvchanligi yoki bilim yetishmasligiga tayanadi. Shu sababli, xavfsizlik bo‘yicha xodimlarni muntazam ravishda o‘qitish, real vaqtda ogohlantirish tizimlari joriy etish va foydalanuvchi ongini oshirish bu turdagi hujumlarga qarshi eng samarali choradir.

4. **Ichki tahdidlar (Insider Threats):** Ichki tahdidlar axborot xavfsizligidagi eng murakkab va ko‘p e’tiborni talab qiladigan tahdidlar sirasiga kiradi. Ular tashkilot ichida ishlovchi shaxslar — xodimlar, pudratchilar yoki vaqtinchalik ishchilar tomonidan sodir etiladi. Ushbu tahdidlar ataylab (yovuz niyat bilan) yoki bexosdan (bilmasdan) yuzaga kelishi mumkin. Ichki tahdidlar tashqi hujumchilarga qaraganda ko‘proq zarar yetkazish salohiyatiga ega, chunki xodimlar ichki tizimlarga to‘liq yoki qisman kirish huquqiga ega bo‘ladi.

Ichki tahdidlarning turlari quyidagilardan iborat:

- **Ataylab zarar yetkazuvchi ichki tahdidlar:** Bu holatlarda xodimlar maqsadli ravishda ma’lumotlarni o‘g‘irlaydi, o‘chiradi yoki tarmoqni buzadi. Masalan, tashkilotdan norozi bo‘lgan sobiq xodimlar yoki raqobatchilar bilan til biriktirgan hodimlar tomonidan amalga oshiriladi.
- **Bexabar ichki tahdidlar:** Bu turdagi tahdidlar xodimlarning yetarli bilimga ega emasligi yoki e’tiborsizligi sababli yuzaga keladi. Masalan, zararli havolani bosib qo‘yish, parollarni notog‘ri saqlash yoki USB qurilma orqali zararli dasturni tizimga kiritish.
- **Xodimlar ustidan tahdidlar:** Bu holatda hujumchi xodimni shantaj yoki pora orqali o‘z foydasiga ishlashga majbur qiladi. Bu turdagi ichki tahdidlar juda murakkab va aniqlash qiyin bo‘ladi.

Ichki tahdidlarning xavfini kamaytirish uchun quyidagi choralar ko‘rilishi lozim:

1. **Kirishni cheklash (Access Control):** Har bir xodimga faqat o‘z vazifasini bajarish uchun zarur bo‘lgan ma’lumot va tizimlarga kirish huquqi berilishi kerak. "Minimal huquqlar tamoyili" (Principle of Least Privilege) asosiy yondashuvdir.

2. **Faoliyatni monitoring qilish:** Xodimlarning faoliyatini doimiy ravishda nazorat qilish, tizimga kirish tarixini saqlash va tahlil qilish orqali noan'anaviy xatti-harakatlar erta aniqlanishi mumkin.

3. **Xavfsizlik siyosatlari va tartib-qoidalari:** Ichki tahdidlar haqida doimiy ravishda ma'lumot berish, xavfsizlik protokollariga rioya etilishini qat'iy nazorat qilish.

4. **Xodimlarni skrining qilish:** Ishga qabul qilish jarayonida xodimlarning fonini tekshirish, ayniqsa yuqori darajadagi kirish huquqlariga ega bo'ladigan pozitsiyalar uchun.

5. **Xavfsizlik bo'yicha madaniyatni rivojlantirish:** Xodimlarga axborot xavfsizligining ahamiyati va o'z harakatlarining oqibatlari haqida doimiy ravishda tushuntirish va treninglar o'tkazish.

Ichki tahdidlar ko'pincha yillar davomida sezilmay yurishi mumkin va katta moliyaviy yoki obro' yo'qotishiga olib keladi. Shu bois, bu xavf turiga qarshi strategik yondashuv va texnologik hamda inson omilini qamrab olgan muvozanatli boshqaruv tizimi zarur hisoblanadi.

5. **Axborot manipulyatsiyasi va dezinformatsiya:** Axborot manipulyatsiyasi va dezinformatsiya zamonaviy axborot urushlarining eng kuchli vositalaridan biridir. Bu hujumlar orqali haqiqiy yoki soxta axborot turli yo'llar bilan buzib talqin qilinadi, maqsad esa jamoatchilik fikrini shakllantirish, qaror qabul qilish jarayonlariga aralashish yoki raqib tuzilmalarga psixologik va siyosiy bosim o'tkazishdan iborat bo'ladi.

Dezinformatsiya hujumlari ko'pincha quyidagi maqsadlarda qo'llaniladi:

- **Siyosiy manipulyatsiya:** Saylovlar, siyosiy kampaniyalar yoki norozilik harakatlari oldidan ijtimoiy tarmoqlar, bot tarmoqlari va soxta akkauntlar orqali noto'g'ri ma'lumotlar tarqatiladi.
- **Iqtisodiy zarar yetkazish:** Investitsiya qarorlariga ta'sir ko'rsatish, bozorlarda beqarorlikni yuzaga keltirish yoki kompaniya obro'sini tushirish uchun noto'g'ri axborotlar targ'ib qilinadi.
- **Ijtimoiy bo'linish yaratish:** Millatlararo, diniy yoki ijtimoiy qatlamlar orasidagi ishonchni buzish uchun yolg'on xabarlar, montaj qilingan tasvirlar yoki noto'g'ri kontekstda olingan ma'lumotlar tarqatiladi.

Dezinformatsiya vositalari quyidagilar bo'lishi mumkin:

- **Deepfake texnologiyasi:** Mashina o'rganish algoritmlaridan foydalanib, mashhur shaxslarning soxta videolari yoki audiosini yaratish orqali yolg'on axborot realdek ko'rsatib beriladi [8].
- **Soxta yangiliklar saytlari (Fake news portals):** Rasmiy yangilik saytlariga o'xshash ko'rinishdagi saytlarda yolg'on va noto'g'ri axborotlar chop etiladi.
- **Bot tarmoqlari va troll fabrikalari:** Ijtimoiy tarmoqlarda noto'g'ri axborotlarni ko'p miqdorda tarqatish va uni mashhurlashtirish uchun avtomatlashtirilgan akkauntlardan foydalaniladi.
- **Memlar va vizual kontent:** O'ta qisqa, ta'sirchan, lekin noto'g'ri yoki kontekstdan chiqarilgan tasvirlar orqali ijtimoiy psixologik ta'sir o'tkaziladi.

Bunday hujumlardan himoyalanish uchun quyidagi choralar muhim:

1. **Axborot manbalarini tekshirish odatini shakllantirish:** Har qanday axborot manbasining ishonchliligi va kontekstini tekshirishni odatga aylantirish.

2. **Media savodxonlikni oshirish:** Fuqarolarni ijtimoiy tarmoqlardagi yolg‘on axborotlarni aniqlash, farqlash va ularga nisbatan tanqidiy yondashishga o‘rgatish.

3. **AI asosidagi kontent verifikatsiyasi vositalari:** Raqamli kontent (foto, video, matn)ning haqiqiyligini aniqlashga mo‘ljallangan algoritmlardan foydalanish [9].

4. **Ijtimoiy tarmoqlarda monitoring va xabar berish tizimlari:** Ijtimoiy tarmoqlarda yolg‘on yoki manipulyativ kontentni avtomatik aniqlaydigan va foydalanuvchilarni ogohlantiradigan vositalar joriy etish.

Axborot manipulyatsiyasi va dezinformatsiya hujumlari jamiyatga uzoq muddatli salbiy ta’sir ko‘rsatadi. Shu sababli ularni aniqlash va bartaraf etish har bir fuqaro, jurnalist, tashkilot va davlat tuzilmalari zimmasiga tushadigan muhim vazifadir.

6. **Tashqi qurilmalar orqali hujumlar:** Tashqi qurilmalar orqali amalga oshiriladigan axborot hujumlari texnik jihatdan oddiy tuyulsa-da, ular juda samarali va xavfli bo‘lishi mumkin. Bu turdagi hujumlar odatda foydalanuvchi yoki tizimga jismonan yaqinlikda bo‘lgan holatlarda qo‘llaniladi va ko‘pincha oflayn (air-gapped) tizimlarga qarshi yo‘naltiriladi. Hujumchi maqsadli tizimga USB fleshka, tashqi qattiq disk, SD-karta yoki boshqa tashqi qurilmalar orqali zararli dastur kiritadi.

Eng ko‘p uchraydigan tashqi qurilma asosidagi hujumlar:

- **USB Rubber Ducky:** Bu qurilma tashqi ko‘rinishidan oddiy USB fleshkaga o‘xshaydi, lekin amalda kompyuterga ulangan zahoti o‘zini klaviatura sifatida tanishtirib, avtomatik tarzda buyruqlarni bajaradi. Masalan, buyruqlar satriga zararli kod kiritish orqali tizimni egallab olish mumkin.
- **BadUSB:** USB qurilmasining mikrodasturiy (firmware) darajasini o‘zgartirib, uni zararli vositaga aylantirish usuli. Bu holatda antivirus dasturlari ko‘pincha hujumni aniqlay olmaydi, chunki u dastlabki fayl tizimini emas, USB apparatini ekspluatatsiya qiladi.
- **Autorun zararli fayllari:** USB qurilmaga joylashtirilgan autorun.inf fayli orqali foydalanuvchi qurilmani ochgan zahoti zararli dastur avtomatik ishga tushiriladi.
- **Soxta tashqi qurilmalar:** Tashqi ko‘rinishda zaryadlovchi, adapter yoki boshqa texnik uskuna ko‘rinishidagi qurilmalarda zararli mikrosxemalar joylashtiriladi. Ular kompyuterga ulangan vaqtda josuslik, ma’lumot o‘g‘riligi yoki boshqa zararli amallarni bajara boshlaydi.

Tashqi qurilmalar orqali amalga oshiriladigan hujumlardan himoyalanish uchun quyidagi chora-tadbirlar muhim:

1. **Begona qurilmalarni ulmaslik siyosati:** Tashkilotlarda noma’lum yoki shaxsiy USB qurilmalarni korporativ kompyuterlarga ulashni qat’iyan man etish kerak.

2. **USB portlarni cheklash:** Tizimlarda USB portlar faolligini dasturiy yoki apparat darajasida nazorat qilish, faqat ruxsat etilgan qurilmalargagina kirish imkoni berish.

3. **Zararli qurilmalarga qarshi skanerlovchi vositalar:** USBGuard, Endpoint Protector kabi xavfsizlik vositalari yordamida ulanuvchi qurilmalarni avtomatik tahlil qilish.

4. **Foydalanuvchilarni xabardor qilish:** Xodimlarga tashqi qurilmalar orqali tahdidlar haqida tushuntirish berish, ehtiyotkorlikni oshirish [6, 88-b.].

5. **Zararsiz alternativlar yaratish:** Fayl almashinuvi uchun xavfsiz korporativ xizmatlar (masalan, ichki fayl serverlari, bulutli xizmatlar) dan foydalanish.

Tashqi qurilmalar orqali hujumlar, ayniqsa sanoat tarmoqlari, harbiy tizimlar yoki moliyaviy institutlar kabi yuqori xavfsizlik talab etiladigan muassasalarda jiddiy xavf

tug‘diradi. Shu bois bu sohada texnik nazorat bilan bir qatorda xavfsizlik madaniyatini ham shakllantirish muhimdir.

7. **Mobil va IoT hujumlari:** Mobil qurilmalar va internetga ulangan aqlli qurilmalar (kameralar, televizorlar, printerlar va boshqalar) orqali foydalanuvchi faoliyatini kuzatish, ularning xavfsizlik zaifliklaridan foydalanish keng tarqalgan. Bu usullar orasida man-in-the-middle (MITM) hujumlari, Bluetooth orqali josuslik va qurilmalarga ruxsatsiz kirish misol bo‘la oladi.

Shu tarzda, axborot hujumlarining har bir turi o‘ziga xos xavf-xatarlarga ega bo‘lib, ularning har biri chuqur tahlil va kompleks himoya choralari ishlab chiqilishini talab qiladi.

Himoyalanish strategiyalari Axborot hujumlaridan samarali himoyalanish kompleks yondashuvni talab etadi. Quyidagi strategiyalar eng dolzarb va amaliy hisoblanadi:

1. **Texnik choralar:** Xavfsizlik devorlari (firewall), antivirus va antimalware tizimlari, ikki bosqichli autentifikatsiya (2FA), IDS/IPS tizimlari (kirishni aniqlash va oldini olish tizimlari), tarmoq monitoringi, xavfsizlikni boshqarish platformalari (SIEM).

2. **Ma’lumotlarni shifrlash:** Transport darajasida (TLS, VPN) va ma’lumot saqlash darajasida (AES, RSA) kuchli kriptografik algoritmlar yordamida ma’lumotlar shifrlanadi. Bu vosita maxfiylik, yaxlitlik va autentiklikni ta’minlaydi.

3. **Xodimlarni o‘qitish va xavfsizlik siyosatlari:** Kiberxavfsizlik bo‘yicha doimiy treninglar, testlar va soxta phishing hujumlari orqali tayyorgarlik. Xodimlar har bir xavfga qanday javob berishni, shubhali xatti-harakatlarni qanday aniqlashni bilishi lozim.

4. **Zaxira nusxalar va tiklash rejasi:** Muhim ma’lumotlar muntazam zaxiralab borilishi, zaxiralar alohida, himoyalangan muhitda saqlanishi va tezkor tiklash rejalari mavjud bo‘lishi lozim. Bu chora ransomware va ma’lumot yo‘qolishiga qarshi muhim hisoblanadi.

5. **Xalqaro standartlarga muvofiqlik:** ISO/IEC 27001, NIST Cybersecurity Framework, COBIT kabi xalqaro standartlar va metodologiyalar asosida tashkilotlar axborot xavfsizligi boshqaruv tizimini shakllantirishlari va muntazam auditlardan o‘tishlari kerak.

Xulosa qiladigan bo‘lsak, axborot hujumlari bugungi kunda har bir jamiyat, tashkilot va shaxsning raqamli hayotida doimiy va dinamik tahdid bo‘lib qolmoqda. Bu hujumlar nafaqat texnik darajadagi buzilishlarga, balki psixologik, iqtisodiy va siyosiy beqarorliklarga ham olib kelmoqda. Shuning uchun axborot xavfsizligini ta’minlash biror bir sohaga tegishli muammo emas, balki har tomonlama yondashuvni talab qiladigan ko‘p qirrali vazifadir.

Maqolada ko‘rib chiqilganidek, zararli dasturlar, xakerlik hujumlari, ijtimoiy muhandislik, ichki tahdidlar, dezinformatsiya, tashqi qurilmalar orqali tahdidlar va IoT qurilmalar xavflari – bularning barchasi o‘ziga xos xususiyatlarga ega va har biri uchun maxsus himoya strategiyalarini talab qiladi. Yagona yondashuv emas, balki qatlamli (multi-layered) mudofaa choralari eng samarali natija beradi.

Samarali himoyalanish quyidagi asosiy tamoyillarga tayanadi:

- ilg‘or texnologik vositalardan foydalanish;
- xodimlarning doimiy o‘quv-tayyorlov jarayonlari;
- xavfsizlik siyosatlarining qat’iy bajarilishi;
- real vaqtda monitoring va tahlil;
- xalqaro standartlarga muvofiqlik;
- madaniyat va ong darajasida xavfsizlikni anglash.

Shuningdek, davlat darajasida axborot xavfsizligi strategiyalarining ishlab chiqilishi, raqamli qonunchilikning rivojlantirilishi, sohaning monitoringi va sertifikatlash tizimlari orqali huquqiy asoslar mustahkamlab borilishi kerak. Bugungi raqamli davrda axborotga oid tahdidlar kundalik hayotning ajralmas qismiga aylanmoqda. Texnik va psixologik hujumlar, zararli dasturlar, dezinformatsiya, ichki xodimlar orqali yuzaga keladigan xavflar – bularning barchasiga qarshi samarali choralar ko‘rilishi zarur. Yagona yechim sifatida qatlamli himoya, doimiy monitoring, zamonaviy texnologiyalardan foydalanish va xodimlar ongini oshirish taklif etiladi. Axborot xavfsizligini ta’minlash har bir tashkilot va shaxsning ustuvor vazifasidir.

Foydalanilgan adabiyotlar ro‘yxati:

1. Solovyev, D. A. "Kiberxavfsizlik asoslari." Moskva, 2020
2. Anderson, R. "Security Engineering: A Guide to Building Dependable Distributed Systems." Wiley, 2021
3. Uzbekistan Respublikasi Milliy axborot xavfsizligi konsepsiyasi, 2022
4. Schneier, B. "Secrets and Lies: Digital Security in a Networked World." Wiley,
5. CERT Uzbekistan – https://www.cert.uz
6. “Kiberxavfsizlik” fanidan ma’ruza matnlari, TATU, 2023
7. OWASP – https://owasp.org
8. Kaspersky Cybersecurity Encyclopedia – https://encyclopedia.kaspersky.com
9. OpenAI ChatGPT modeli – https://chat.openai.com