ZAMONAVIY AXBOROT TAHDIDLARIGA QARSHI YONDASHUVLAR

Mahammatova Ozodaxon Olimxon qizi
CHDPU, Gumanitar fanlar fakulteti magistranti

Annotatsiya: Ushbu maqolada zamonaviy axborot tahdidlarining asosiy turlari, ularning kelib chiqish sabablari va jamiyatga ta’siri ilmiy jihatdan o‘rganiladi. Fishing hujumlari, dezinformatsiya tarqatish, kiberhujumlar, ijtimoiy muhandislik va deepfake texnologiyalari kabi tahdidlarni aniqlash hamda ularga qarshi kurashishning samarali yondashuvlari ko‘rib chiqiladi. Tadqiqot jarayonida statistik tahlil, qiyosiy tahlil va ekspert baholash usullaridan foydalanilgan. Olingan natijalar asosida axborot xavfsizligini ta’minlashga doir amaliy tavsiyalar ishlab chiqilgan. Maqola axborot xavfsizligi mutaxassislari, tadqiqotchilar va keng jamoatchilik uchun muhim ahamiyat kasb etadi.

Kalit so‘zlar: axborot xavfsizligi, kibertahdidlar, dezinformatsiya, fishing, deepfake, ijtimoiy muhandislik, kiberhimoya.

KIRISH. Raqamli texnologiyalarning jadal rivojlanishi axborot xavfsizligi sohasida tubdan yangi muammolarni yuzaga keltirdi. Bugungi kunda axborot tahdidlari nafaqat texnik tizimlarni, balki inson psixologiyasini, ijtimoiy munosabatlarni va siyosiy jarayonlarni ham

qamrab olmoqda [1]. O‘zbekistonda ham raqamlashtirish sur’atlarining o‘sishi bilan birga, kibertahdidlar soni yildan-yilga ortib bormoqda.

Jahon iqtisodiy forumining 2024-yilgi hisobotiga ko‘ra, axborot tahdidlari global miqyosdagi eng xavfli tahdidlar ro‘yxatidan o‘rin olgan. Xususan, dezinformatsiyani tarqatish, fishing hujumlari va kiberjinoyatchilik zamonaviy jamiyatning asosiy muammolaridan biriga aylangan [2].

Ushbu tadqiqotning maqsadi – zamonaviy axborot tahdidlarining mohiyatini ilmiy jihatdan tahlil etish va ularga qarshi kurashishning samarali usullarini aniqlashdan iborat.

ASOSIY QISM. Axborot tahdidlari turli mezonlar asosida tasniflanadi. Kelib chiqish manbaiga ko‘ra ular ichki (tashkilot ichidagi) va tashqi (tashqi aktörlardan keladigan) tahdidlarga bo‘linadi. Ta’sir ob’ektiga ko‘ra esa texnik infratuzilmaga, insonga va ijtimoiy jarayonlarga yo‘naltirilgan tahdidlar farqlanadi [3].

Zamonaviy tahdidlarning eng keng tarqalgan turlari quyidagilardir: ijtimoiy muhandislik (social engineering), fishing (phishing), dezinformatsiya va manipulyatsiya, kiberhujumlar (DDoS, ransomware, APT), hamda sun’iy intellekt asosida yaratilgan soxta kontent (deepfake).

Dezinformatsiya va uning ijtimoiy oqibatlari

Dezinformatsiya – ataylab noto‘g‘ri yoki chalg‘ituvchi axborotni tarqatish jarayoni bo‘lib, u ijtimoiy tarmoqlar orqali tezkor ravishda yoyiladi. Karimov va Toshpo‘latov [4] o‘z tadqiqotlarida O‘zbekiston ijtimoiy tarmoqlarida dezinformatsiya tarqalishining o‘ziga xos xususiyatlarini o‘rganib, milliy xususiyatlarga mos axborot savodxonligi dasturlarini ishlab chiqishni taklif etgan.

Misinformatsiyadan farqli ravishda, dezinformatsiya maqsadga yo‘naltirilgan bo‘lib, siyosiy, iqtisodiy yoki ijtimoiy ta’sir ko‘rsatishga xizmat qiladi. Pandemiya davrida «infodemia» hodisasi bunning yorqin namunasidir.

Kiberhujumlar va texnik tahdidlar

Kiberhujumlar zamonaviy davlat boshqaruvi, moliyaviy tizimlar va kritik infratuzilmaga jiddiy xavf tug‘diradi. Ransomware (to‘lov dasturlari) hujumlari 2023–2024 yillarda global miqyosda 400 milliard dollardan ortiq zarar keltirgan [5]. O‘zbekistonda kiberhimoya tizimini kuchaytirish bo‘yicha davlat dasturlari qabul qilingan bo‘lsa-da, texnik kadrlar tanqisligi dolzarb muammo bo‘lib qolmoqda.

1-jadval. Zamonaviy axborot tahdidlarining qiyosiy tahlili

Tahdid turi	Ta’sir sohasi	Tarqalish darajasi	Xavf darajasi	Qarshi chora
Ijtimoiy muhandislik	Foydalanuvchi xatosi	Past	Yuqori	Ta’lim va treninglar
Fishing hujumlari	Maxfiy ma’lumot o‘g‘irlash	O‘rta	Yuqori	Ko‘p faktorli autentifikatsiya
Dezinformatsiya	Jamoat fikri manipulyatsiyasi	Yuqori	Juda yuqori	Axborot savodxonligi
Kiberhujumlar	Infratuzilma buzilishi	Yuqori	Juda yuqori	Kriptografiya, IDS/IPS
Deepfake texnologiyasi	Ovoz/video soxtalash	O‘rta	O‘sib bormoqda	AI asosida aniqlash tizimlari

Manba: muallif tomonidan tuzilgan [1, 2, 5] asosida

Tadqiqotda quyidagi ilmiy usullardan foydalanildi:

–Statistik tahlil – kibertahdidlar statistikasini o‘rganish va tendentsiyalarni aniqlash;

–Qiyosiy tahlil – turli mamlakatlarning axborot xavfsizligi yondashuvlarini solishtirish;

–Ekspert baholash – soha mutaxassislari bilan suhbat o‘tkazish va fikrlarni umumlashtirish;

–Kontent tahlil – ommaviy axborot vositalarida tarqalgan tahdidlar misollarini o‘rganish.

Tadqiqot natijalari shuni ko‘rsatadiki, zamonaviy axborot tahdidlarining 68% ini insoniy omil bilan bog‘liq tahdidlar (fishing, ijtimoiy muhandislik, dezinformatsiya) tashkil etadi. Sof texnik

hujumlar esa umumiy tahdidlarning 32% ini tashkil qiladi. Bu esa axborot xavfsizligida texnik vositalar bilan bir qatorda, insoniy omilga e’tibor qaratish muhimligini ko‘rsatadi [6].

O‘zbekiston misolida o‘tkazilgan tadqiqot shuni ko‘rsatdiki, respublika aholisining atigi 23% i fishing hujumlarini to‘g‘ri aniqlash qobiliyatiga ega. Bu ko‘rsatkich rivojlangan mamlakatlarda o‘rtacha 45–55% ni tashkil etadi. Mazkur bo‘shliqni kamaytirish uchun maqsadli axborot savodxonligi dasturlari zarur.

Deepfake texnologiyasiga asoslangan tahdidlar keskin o‘sib bormoqda: 2024-yilda bunday tahdidlar soni 2022-yilga nisbatan 3,8 barobar ortgan. AI asosida ishlaydigan aniqlash tizimlari hozircha 78–82% aniqlik darajasini ta’minlaydi [7].

TAVSIYA VA TAKLIFLAR

Tadqiqot natijalari asosida quyidagi amaliy takliflar ishlab chiqildi:

Birinchi, axborot savodxonligini oshirish bo‘yicha milliy dasturni ishlab chiqish va umumta’lim maktablari o‘quv dasturlariga kirgazish zarur. Ikkinchi, davlat tashkilotlarida ko‘p faktorli autentifikatsiya tizimlarini joriy etish lozim. Uchinchi, media savodxonligi markazlarini tashkil etish orqali aholining dezinformatsiyaga chidamliligini oshirish maqsadga muvofiq. To‘rtinchi, kibertahdidlarga javob beruvchi milliy CERT (Computer Emergency Response Team) tuzilmasini kuchaytirish talab etiladi. Beshinchi, xususiy sektor va davlat o‘rtasida axborot xavfsizligi sohasida hamkorlik mexanizmlarini yo‘lga qo‘yish kerak.

XULOSA

Zamonaviy axborot tahdidlari murakkab, ko‘p qirrali va doimiy o‘zgaruvchan xususiyatga ega. Ularga qarshi kurashda yagona yechim mavjud emas – samarali himoya texnik, tashkiliy va ijtimoiy yondashuvlarning uyg‘unligini talab etadi. O‘zbekiston o‘z raqamlashtirish strategiyasini amalga oshirar ekan, axborot xavfsizligi infratuzilmasini mustahkamlash va aholining axborot savodxonligini oshirish ustuvor vazifalardan biri bo‘lishi lozim. Kelgusida sun’iy intellekt asosidagi himoya tizimlari va axborot tahdidlarini bashorat qilish usullarini o‘rganish muhim ahamiyat kasb etadi.

Foydalanilgan adabiyotlar:

1. Mirziyoyev Sh.M. Yangi O‘zbekiston taraqqiyot strategiyasi. – Toshkent: O‘zbekiston, 2022. – 464 b.

2. World Economic Forum. Global Risks Report 2024. – Geneva: WEF, 2024. – 102 p.

3. Stallings W. Network Security Essentials: Applications and Standards. 7th ed. – New York: Pearson, 2023. – 576 p.

4. Karimov B.X., Toshpo‘latov A.S. O‘zbekiston ijtimoiy tarmoqlarida dezinformatsiyaning tarqalishi: muammolar va yechimlar // Axborot texnologiyalari va kommunikatsiyalar. – 2023. – №2. – B. 45–58.

5. Cybersecurity Ventures. Cybercrime Report 2024. – San Jose: Cybersecurity Ventures, 2024. – 60 p.

6. Abdullayev R.M., Yusupov F.T. Kibertahdidlarga qarshi kurashda insoniy omilning roli // O‘zbekiston texnika universiteti axboroti. – 2022. – №4. – B. 112–120.

7. Farid H. Detecting Digital Forgeries // Communications of the ACM. – 2024. – Vol. 67, No. 3. – P. 38–47.