SUN'IY INTELLEKT DAVRIDA IJTIMOIY INJENERIYA: OLIY TA'LIM XODIMLARI UCHUN KIBERXAVFSIZLIK BO'YICHA XABARDORLIK MODELI

Qulliyev Javohirbek G'anijon o'g'li
Buxoro davlat pedagogika instituti
javohr00@gmail.com

Annotatsiya. *Mazkur maqolada sun'iy intellekt (SI) vositalari ijtimoiy injeneriya hujumlarini qanday kuchaytirayotgani tahlil qilinadi va oliy ta'lim muassasalarining AT bo'lmagan xodimlari uchun kiberxavfsizlik bo'yicha xabardorlikni oshirishning amaliy modeli taklif etiladi. "Tanib ol – Tekshir – Himoyalan – Xabar ber" deb nomlangan model xodim ko'nikmalarini, amaliy mashqlarni va baholash mezonlarini o'zaro bog'laydi. Model sakkiz darsdan iborat kurs tuzilmasiga asos qilib olingan.*

Kalit so'zlar: *ijtimoiy injeneriya, sun'iy intellekt, kiberxavfsizlik, xabardorlik, fishing, oliy ta'lim.*

Аннотация. *В статье анализируется, как инструменты искусственного интеллекта (ИИ) усиливают атаки социальной инженерии, и предлагается практическая модель повышения осведомлённости в области кибербезопасности для сотрудников вузов, не являющихся ИТ-специалистами. Модель «Распознай – Проверь – Защити себя – Сообщи» связывает навыки сотрудника, практические упражнения и критерии оценки. Модель положена в основу структуры курса из восьми занятий.*

Ключевые слова: *социальная инженерия, искусственный интеллект, кибербезопасность, осведомлённость, фишинг, высшее образование.*

Abstract. *The article analyzes how artificial intelligence (AI) tools strengthen social engineering attacks and proposes a practical cybersecurity awareness model for non-IT staff of higher education institutions. The model, called "Recognize – Verify – Protect – Report", links staff skills, practical exercises and assessment criteria. It is used as the basis for the structure of an eight-lesson course.*

Keywords: *social engineering, artificial intelligence, cybersecurity, awareness, phishing, higher education.*

Kirish. So‘nggi yillarda sun’iy intellekt texnologiyalari, xususan, katta til modellari hamda ovoz va tasvir sintezi vositalari keng foydalanuvchilar uchun ochiq bo‘ldi. Bu vositalar kiberjinoyatchilar qo‘lida ham samarali quralga aylanmoqda. Kiberxavfsizlik bo‘yicha xalqaro hisobotlar ma’lumotlar buzilishi holatlarining katta qismida inson omili ishtirok etishini ko‘rsatadi [9]. Hujumchilar ko‘pincha tizimni emas, foydalanuvchini “buzadi”; bu yondashuv ijtimoiy injeneriya deb ataladi [1; 2].

Avval soxta xabarni imlo va uslub xatolaridan tanish mumkin edi, katta til modellari bu xatolarni deyarli bartaraf etdi. Til modellari yordamida tayyorlangan fishing xatlari mutaxassislar yozgan xatlar bilan taqqoslanadigan darajada samarali bo‘lishi mumkinligi ko‘rsatilgan [7]. Natijada “xatosiz matn – ishonchli matn” degan eski qoida ishlamay qoldi.

Oliy ta’lim muassasalari xodimlari bu jihatdan alohida e’tiborga loyiq. Ular shaxsiy ma’lumotlar va davlat axborot tizimlari bilan ishlaydi, ko‘pchiligi esa IT mutaxassisi emas. Maqolaning maqsadi sun’iy intellekt davrida ijtimoiy injeneriya xavflarini tahlil qilish va IT bo‘lmagan oliy ta’lim xodimlari uchun kiberxavfsizlik bo‘yicha xabardorlikni oshirishning amaliy modelini taklif etishdir.

Asosiy qism. Tadqiqot loyihalash yo‘nalishidagi tahliliy usulga asoslangan: ijtimoiy injeneriya bo‘yicha manbalar tahlil qilindi, oliy ta’lim xodimlarining ish jarayonlari uchun xos xavf stsenariylari ajratildi va ular asosida xabardorlik modeli ishlab chiqildi. Maqolada empirik natijalar emas, loyihalash natijasi bayon etiladi.

1. Sun’iy intellekt bilan kuchaytirilgan xavflar

Birinchi xavf – shaxsiylashtirilgan fishingdir. Hujumchi muassasa veb-sayti, ijtimoiy tarmoqlar va ochiq hujjatlardan xodim haqida ma’lumot yig‘adi, til modeli esa shu ma’lumotga mos, aniq shaxsga yo‘naltirilgan xat yoki xabarni bir necha soniyada tayyorlaydi. Bunday xabar o‘zbek yoki rus tilida grammatik xatolarsiz yoziladi va rasmiy uslubni yaxshi taqlid qiladi. Fishing hujumlarining bosqichlari [6] da tasniflangan.

Ikkinchi xavf – ovoz va video soxtalashtirish (dipfeyk). Rahbar nomidan “shoshilinch” qo‘ng‘iroq qilib, hujjatni imzolashni, pul o‘tkazishni yoki tasdiqlash kodini aytishni so‘rash mumkin. Bunday soxtalashtirish xavfi [5] da tahlil qilingan.

Uchinchi xavf – messenjerlar va davlat xizmatlari nomidan qilinadigan hujumlardir. Bunda SMS orqali kelgan bir martalik kodni yuborish, soxta

havolada login va parolni kiritish so‘raladi. Bunday hujumlar ishonch, hokimiyat va shoshilinchlik kabi ijtimoiy-psixologik ta’sir tamoyillariga tayanadi [4].

2. Oliy ta’lim xodimlari nima uchun maqsadli nishon bo‘ladi

Birinchidan, oliy ta’lim muassasasi katta hajmdagi shaxsiy ma’lumotlarni saqlaydi: talabalar, o‘qituvchilar, kadrlar va ilmiy loyihalar bo‘yicha ma’lumotlar. Ikkinchidan, xodimlar elektron raqamli imzo (ERI), OneID kabi yuqori huquqli vositalardan foydalanadi. Uchinchidan, ish yuklamasi yuqori bo‘lgan sharoitda xodim tez qaror qabul qiladi, rasmiy “buyruq” yoki “rahbar iltimosi” esa tekshirilmasdan bajarilishi mumkin.

Kiberxavfsizlik sohasidagi munosabatlar O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni bilan tartibga solinadi [8]. Xalqaro amaliyotda xabardorlik dasturlari rolga xos va uzluksiz bo‘lishi tavsiya etiladi [3].

3. Taklif etilgan model: Tanib ol – Tekshir – Himoyalan – Xabar ber

Model to‘rt bosqichdan iborat. Har bir bosqich xodim ko‘nikmasi va amaliy mashq bilan bog‘langan (1-jadval).

1-jadval. Xabardorlik modelining bosqichlari

Bosqich	Xodim ko‘nikmasi	Amaliy mashq
Tanib ol	Shoshiltirish, maxfiylikni talab qilish, kod yoki parol so‘rash, odatiy bo‘lmagan kanal kabi belgilarni ajratadi. Matn xatosiz bo‘lishi uni ishonchli qilmasligini biladi.	Haqiqiy va soxta xabarlarni saralash; sun’iy intellekt yozgan xatni tahlil qilish.
Tekshir	So‘rovni mustaqil kanal orqali tasdiqlaydi: rasmiy raqamga qayta qo‘ng‘iroq qiladi, havolani qo‘lda ochadi.	“Ikki kanal qoidasi” bo‘yicha rolli o‘yin: rahbar nomidan kelgan qo‘ng‘iroq.
Himoyalan	Ikki bosqichli autentifikatsiyani yoqadi, parol menejeridan foydalanadi, ERI kalitini va tasdiqlash kodlarini hech kimga bermaydi, qurilmani yangilab turadi.	Shaxsiy hisoblarni tekshirish ro‘yxati bo‘yicha xavfsizlik sozlamalarini tekshirish.
Xabar ber	Gumonli holatni jazolanish qo‘rquvisiz, tez va belgilangan tartibda xabar qiladi.	Hodisa haqida qisqa xabar shaklini to‘ldirish.

Modelning asosiy g‘oyasi shundaki, xodimdan har bir hujum turini yodlash talab qilinmaydi. Sun’iy intellekt vositalari tez o‘zgargani uchun model aniq hujum shakllariga emas, xodimning doimiy harakatlariga tayanadi. “Tekshir” bosqichi eng muhimi, chunki u xabar qanchalik ishonarli ko‘rinmasin, qarorni tashqi tasdiqqa bog‘laydi.

4. Kurs tuzilmasi va baholash

Model sakkiz darsdan iborat kurs va yakuniy amaliy topshiriq shaklida joriy etish uchun mo‘ljallangan. Mavzular: messenjerlar xavfsizligi, OneID va davlat

portallari, ERI kalitini himoyalash, zararli dasturlar, fishing va telefon firibgarligi; yakuniy modul sun'iy intellekt va kiberxavfsizlikka bag'ishlanadi. Har bir dars ma'ruza va qisqa amaliy mashqdan iborat.

Baholash ikki qismdan iborat. Birinchisi – kursdan oldin va keyin o'tkaziladigan bir xil test. Ikkinchisi – amaliy stsenariylar bo'yicha topshiriqlar. Kutilayotgan ko'rsatkichlar: soxta xabarni to'g'ri aniqlash ulushi va hodisa haqida xabar berish vaqti. Fishing simulyatsiyalari faqat xodimlarning roziligi bilan o'tkaziladi, natijalar umumiy tahlil uchun ishlatiladi [3].

5. Cheklovlar

Ishning cheklovlari bor. Model hozircha empirik sinovdan o'tkazilmagan, samaradorligi kursdan oldingi va keyingi natijalarni solishtirgandan keyin aniqlanadi. Xabardorlik doim xavfsiz xatti-harakatga aylanmasligi mumkin, shuning uchun davriy takrorlash zarur. Keyingi bosqichda model bir necha bo'lim xodimlari bilan sinovdan o'tkaziladi.

Xulosa. Sun'iy intellekt ijtimoiy injeneriya hujumlarini shaxsiylashtirilgan va tilda xatosiz qilmoqda. Taklif etilgan "Tanib ol – Tekshir – Himoyalan – Xabar ber" modeli xodim ko'nikmalarini, amaliy mashqlarni va baholashni yagona tizimga bog'laydi va sakkiz darsli kurs tuzilmasiga asos bo'la oladi. Modelning samaradorligi keyingi bosqichda amaliy sinov orqali aniqlanadi.

Foydalanilgan adabiyotlar

1. Mitnick K.D., Simon W.L. The Art of Deception: Controlling the Human Element of Security. – Indianapolis: Wiley, 2002. – 352 p.

2. Hadnagy C. Social Engineering: The Science of Human Hacking. 2nd ed. – Hoboken: Wiley, 2018. – 320 p.

3. Wilson M., Hash J. Building an Information Technology Security Awareness and Training Program. NIST Special Publication 800-50. – Gaithersburg: National Institute of Standards and Technology, 2003.

4. Cialdini R.B. Influence: Science and Practice. 5th ed. – Boston: Pearson Education, 2009.

5. Chesney R., Citron D. Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security // California Law Review. – 2019. – Vol. 107, No. 6. – P. 1753–1819.

6. Alkhalil Z., Hewage C., Nawaf L., Khan I. Phishing Attacks: A Recent Comprehensive Study and a New Anatomy // Frontiers in Computer Science. – 2021. – Vol. 3. – Article 563060.

7. Heiding F., Schneier B., Vishwanath A., Bernstein J., Park P.S. Devising and Detecting Phishing Emails Using Large Language Models // IEEE Access. – 2024. – Vol. 12. – P. 42131–42146.

8. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni, 2022-yil 15-aprel, O‘RQ-764-son. – URL: https://lex.uz

9. Verizon. 2024 Data Breach Investigations Report. – New York: Verizon Business, 2024.