KIBERXAVFSIZLIK VA TILSHUNOSLIK O‘RTASIDAGI BEVOSITA ALOQALAR

Amankeldiyeva Sevinch Maxmud Qizi
Buxoro Davlat Universiteti Filologiya vatillarni o‘qitish: o‘zbek tili 1-kurs talabasi

Anotatsiya: *Kiberxavfsizlik va tilshunoslik bir biriga uzviy aloqador. Ularning yig‘indisi rivojlanayotgan davrning boshlanishidir. Kiberxavfsizlik sohasida til omilining roli, xususan, internet tarmoqlarida uchraydigan matnlar, xabarlar va kommunikatsiya jarayonlarini tahlil qilish orqali turli xil kiberxavflarni aniqlash imkoniyatlari ko‘rib chiqiladi.*

Аннотация: *Кибербезопасность и лингвистика тесно взаимосвязаны. Их совокупность является началом развивающейся эпохи. В сфере кибербезопасности рассматривается роль языкового фактора, в частности возможности выявления различных киберугроз посредством анализа текстов, сообщений и коммуникационных процессов, встречающихся в интернет-сетях.*

Annotation: *Cybersecurity and linguistics are closely interconnected. Their combination marks the beginning of a developing era. In the field of cybersecurity, the role of the linguistic factor is examined, particularly the possibilities of identifying various cyber threats through the analysis of texts, messages, and communication processes found on the internet.*

Kalit so‘zlar: *kiberxavfsizlik, tilshunoslik, ma’lumotlarni shifrlash, elektron pochta manzili, maxsus belgilar, опасност, revange, raqamli texnologiyalar, qisqartmalar, maxfiylik, bloklash, kiberjinoyat, xeshteg, ramzlar, kodlash, xaker, fishing.*

Ключевые слова: *кибербезопасность, лингвистика, шифрование данных, адрес электронной почты, специальные символы, опасность, месть, цифровые технологии, сокращения, конфиденциальность, блокировка, киберпреступление, хэштег, символы, кодирование, хакер, фишинг.*

Keywords: *cybersecurity, linguistics, data encryption, email address, special characters, danger, revenge, digital technologies, abbreviations, confidentiality, blocking, cybercrime, hashtag, symbols, encoding, hacker, phishing.*

Kirish. Kiberxavfsizlik va tilshunoslik o‘rtasida bevosita aloqalar mavjud, ayniqsa, ma’lumotlarni tahlil qilish, shifrlash va xavflarni aniqlash kabi sohalarda. Tillarni avtomatik tanish va tahlil qilish: kiberxavfsizlik sohasidagi tahlilchilarga kiberjinoyatlarni yoki xakerlik urinishlarini aniqlashda tilshunoslik yordam beradi. Masalan, ma’lumotlarni shifrlash, elektron pochtalar yoki ijtimoiy tarmoqlardagi xavfli xabarlarni lingvistik tahlil

qilish orqali ularni avtomatik ravishda aniqlash va xavfni baholash mumkin.[1]

Tabiiy tilni qayta ishlash(Natural Language Processing, NLP): Kiberxavfsizlikda NLP juda muhim ro‘l o‘ynaydi. Mashinalar inson tillarini tushunish va qayta ishlash orqali elektron xatlar, xabarlar va postlardagi tahdidlar va fishing kabi kiberxujumlarni aniqlashga yordam beradi.

Shifrlash (kriptografiya): Tilshunoslik va shifrlash o‘rtasidagi aloqa shifrlar kodlarini yoki xakerlar tomonidan ishlatilgan “ma’lumotlarni yashirish” usullarini ochib berishda ko‘rinadi.

Bunda tilni anglash va uning qoidalarini bilish shifrlarni parchalashga yordam beradi.[5]

Ijtimoiy tarmoqdagi xavfli xabarlarni lingvistik tahlil qilishda bir qator muhim omillarga e’tibor berish lozim. Bu omillar yordamida xavfli kontentni avtomatik aniqlash va tahdidlarni kamaytirish mumkin. Quyida ayrim amallar keltirilgan:

Muhokama: Leksika va so‘z tanlovi: Hujumkor yoki agressiv so‘zlar, tahdid yoki tajovuzni ifoda etuvchi iboralar (masalan, “o‘ldiraman”, “bomba qo‘yaman”). Faxsh yoki qonunga zid so‘zlar va iboralar. Noma’lum yoki foydalaniladigan kodlashtirilgan so‘zlar, masalan, “dark web”da ishlatilishi mumkin bo‘lgan jargonlar. Grammatika va sintaksis: Oddiy jumla tuzilishidagi o‘zgarishlar yoki qasddan adabiy qoidalarni buzish, bu shifrlash yoki yashirin ma’nolarni berishi mumkin.

Tilida no‘g‘on (masalan, xarflarni qasddan noto‘g’ri yozish) yoki so‘zlarni birlashtirish orqali botlar yoki feyk hisoblar tomonidan tarqatiladigan xabarlar. Emotsional ton va kayfiyat: Juda yomon, norozi yoki tahdidli tondagi xabarlar. Majburiy yoki tasir qilishga qaratilgan kontent, ijtimoiy muhandislik hujumlariga yo‘naltirilgan bo‘lishi mumkin. Qoliplarni aniqlash (patternlarni tanib olish):

Tahdidlar yoki xavfli xabarlarni ko‘pincha takrorlovchi qoliplar bo‘yicha aniqlash mumkin. Masalan, bir xil iboralar va so‘zlar ko‘p marta yoki har xil guruhlarda takrorlansa. Yolg‘on ma’lumot yoki provokatsion ma’lumot tarqatish uchun ma’lum bir matn shablonlaridan foydalaniladi.

Konteks va metama’no: Har bir so‘z va iboraning ma’nosi uning kontekstida aniqlanadi. Masalan, biror kino yoki ijtimoy voqea haqidagi

tahlil shunday kontekstga asoslangan bo‘lishi mumkin. Hatto qarama-qarshi ma’noga ega bo‘lgan yumor yoki sarkazm ham tahdidlar yoki xavfli kontendni yashirishi mumkin.

Xeshteglar va aloqa elementlari: Xeshteglar va ularning qanday ega ekanligiga e’tibor berish kerak. Masalan, #опасност yoki #revange kabi xeshteglar xavfli yoki radikal harakatlarni bildirishi mumkin. O‘zaro aloqa elementlari (bog‘liq, akkauntlar yoki postlar) orqali xavfli xabarlar tarmoqda qanday tarqalyotganini tushunish.

Harf yoki ramzlar almashtirilishi (obfuscation): Xakerlar yoki kiberjinoyatchilar foydalanishi mumkin bo‘lgan usullardan biri bu harflar va raqamlar yoki boshqa

simvollarni aralashtirib yozish (masalan, “0” o‘rniga “o”, “@” o‘rniga “a”). Bu qidiruv algoritlarini aldash uchun ishlatiladi.

Maqsadli auditoriyaga ta’sir qilish: Yoshlar yoki turli ijtiomiy qatlamlarga qaratilgan xavfli yoki ekstremistik kontentlarni faxmlash uchun tilshunoslar kantentning qaysi auditoriyaga qaratilganligini ham tahlil qiladilar. Masalan, harflar yoki ramzlarni almashtirish (обфускация) usuli kiberjinoyatchilar tomonidan xabarlar va ma’lumotlarni yashirish yoki qidiruv algoritmlarini aldash maqsadida keng qo‘llaniladi. Bu usulda standard harflar, raqamlar yoki boshqa simvollar bilan almashtiriladi, lekin o‘quvchi xabarni o‘qishda qiyinchilik sezmaydi.[2]

Quyida buning ayrim misollari keltirilgan:

Qo‘llashdagi misollar:

“H3II0” YOKI “H3110” - “HELLO” so‘zining harf va raqamlar bilan almashtirilgan shakli.

“P@ssw0rd” - “Password” so‘zining xarf va raqamlar bilan almashtirilgan shakli.

“5ecur1ty” - “Security” so‘zining “s” o‘rnida “5”, “I” o‘rnida “1” bilan almashtirib yozish.

Kodlashtirilgan so‘zlar:

“1nv1te” - “Invite” so‘zini “I” o‘rniga “1” bilan yozish. “10v3” - “Love” so‘zining raqamlar bilan almashtirilgan shakli.

“g00gl3” - “google” so‘zining raqamlar bilan yozilgan versiyasi. Harflarni qasddan noto‘g’ri yozish:

“fr33” - “free” so‘zini “e” o‘rniga “3” bilan almashtirib yozish. “ph1sh1ng” - “ Phishing” so‘zini raqamlar bilan almashtirib yozish. [3]

Murakkab ramzlar va simvollar:

“M@yhem” - “Mayhem” so‘zini ramzlar va harflar bilan aralashtirib yozish. Bu kabi opfuskatsiya usullari fishing yoki zararli kodlarni yopishda ham qo‘llaniladi. Ulardan foydalangan xolda kiberxavfsizlik tizimlari yoki filtrlarni chetlab o‘tishga urinishadi, shu bilan insonlarning diqqatini kamaytirishga harakat qiladilar.

Harflarni qasddan noto‘g‘ri yozish (masalan, raqamlar va ramzlar bilar almashtirish) kiberxavfsizlikning to‘g‘ridan to‘g‘ri elementi emas, lekin bu kiberxavfsizlikka taalluqli obfuskatsiya usulining bir qismi hisoblanadi. Bu usul qidiruv sistemalari yoki xavfni aniqlovchi algoritmlardan qochish, zararli yoki xavfli xabarlarni yashirish yoki fishing hujumlarini amalga oshirishda qo‘llaniladi. Quyida xarflarni qasddan noto‘g‘ri yozishning kiberxavfsizlikka qanday tasir qilishini ko‘rsatuvchi omillar keltirilgan:

Fishing hujumlari: Xakerlar yoki kiberjinoyatchilar “fishing” elektron pochtalari xabarlarida harflarni qasddan noto‘g‘ri yozib, odamlarni aldashadi. Masalan, haqiqiy vebsayt nomi “Bank” bo‘lishi kerak, lekin ular “B@nk” yoki

“B4nk” kabi almashtirilgan versiyani yozishi mumkin. Bu foydalanuvchilarni shubxasizlik bilan feyk saytlarga kirishga undaydi. Qidiruv algoritmlarini aldash: Harflarni noto‘g‘ri yozish yordamida kiberjinoyatchilar xavfli kontent yoki zararli xabarlar qidiruv tizimlarida to‘g‘ridan to‘g‘ri aniqlamay qolishiga harak qiladilar. Masalan, “virus” so‘zi o‘rniga “v1ru$” yoki “v!rus” yozish orqali zararli fayllar yoki postlar filtrlardan o‘tib ketishi mumkin. [6]

Maxfiylikni oshirish: Obfuskatsiya usuli orqali zararli kodlar yoki shifrlangan xabarlar foydalaniladi. Harflarni noto‘g‘ri yozish bilan xabarlarni o‘qishni qiyinlashtirish mumkin. Bu ayniqsa zararli dasturlar (malware) va ularning jamoalari o‘rtasidagi aloqa yozishmalarini aniqlashni qiyinlashtiradi.

Spam va botlarning faoliyati: Spam yoki botlar ma’lum bir xizmatlar yoki platformadagi filtrlardan qochish uchun harflarni noto‘g‘ri yozish usulini qo‘llashadi. Bu usul botlarning zararli yoki noqonuniy kontent tarqatish imkoniyatini oshiradi [4].

Xulosa qilib aytganda, ushbu yondoshuv to‘g‘ridan-to‘g‘ri kiberxavfsizlikka tahdid emas, lekin u xavfli kontent va zararli harakatlarni tarqatishda qo‘llaniladigan bir usuldir. Kiberxavfsizlik tizimlari va lingvistik tahlillar bu usularni aniqlash va ularni oldindan himoya qilishga yo‘naltirilgan sohadir

FOYDALANILGAN ADABIYOTLAR

1. Ganiev S.K., Ganiyev A.A., Xudoyqulov Z.T. Kiberxavfsizlik asoslari: O‘quv qo‘llanma /; - T.: “Iqtisod-Moliya”, 2021. - 228 b.
2. Zulxumor Xolmanova. Tilshunoslik nazariyasi [Matn] : darslik, - Toshkent: Shafoat Nur Fayz, 2020. - 256 b.
3. O‘rinbayeva D.B. “Kompyuter lingvistikasi” o‘quv qo‘llanma. - Samarqaand, SamDU nashr, 2020. - 326 b.
4. www.Lex.uz
5. www.intuit.ru
6. www.securtylab.ru