# IJTIMOIY TARMOQLAR ORQALI ZARARLI ILOVALARNI TARQATISH BILAN BOG‘LIQ KIBERJINOYATLARNING OLDINI OLISH, AYOLLAR VA BOLALARGA NISBATAN ZO‘RAVONLIKNING KIBER SHAKLLARI, KRIMINOLOGIK OMILLARI VA INNOVATSION PROFILAKTIKA YECHIMLARI

***U.Sh. Xamraqulov, U.L. Eshonqulov***

**Annotatsiya.** Mazkur maqolada ijtimoiy tarmoqlar va messenjerlar orqali zararli mobil ilovalar, shubhali fayllar hamda xavfli havolalarni tarqatish bilan bog‘liq kiberjinoyatlarning oldini olish masalalari tadqiq etilgan. Tadqiqotning amaliy qismi sifatida Telegram platformasida ishlab chiqilgan @samcyber_102bot avtomatlashtirilgan botining vazifalari, ishlash tamoyili va profilaktik ahamiyati yoritilgan. Shuningdek, raqamli muhitda ayollar va bolalarga nisbatan zo‘ravonlikning kiber shakllari — tahdid, ta’qib, shaxsiy ma’lumotlarni oshkor qilish, firibgarlik, zararli havola yoki ilova orqali nazorat o‘rnatishga urinish kabi xatti-harakatlarning kriminologik xususiyatlari ko‘rib chiqiladi. Profilaktik yondashuvda zararli kontentni jabrlanuvchiga yetib borishidan oldin aniqlash, avtomatik moderatsiya, inson nazorati, raqamli savodxonlik va idoralararo hamkorlikni uyg‘unlashtirish taklif etiladi. Amaliy qismda @samcyber_102bot Telegram guruhlari va kanallarida potensial zararli kontentni aniqlash va belgilangan mezonlar asosida o‘chirishga yo‘naltirilgan vosita sifatida tahlil qilinadi.

**Kalit so‘zlar:** kiberjinoyat, kiberxavfsizlik, ijtimoiy tarmoq, Telegram, zararli ilova, APK, zararli havola, fishing, avtomatik moderatsiya, ayollar, bolalar, kiberzo‘ravonlik, kiber-ta’qib, shaxsiy ma’lumotlar, raqamli xavfsizlik, profilaktika.

## Tadqiqotning maqsadi va vazifalari.

Tadqiqotning asosiy maqsadi — ijtimoiy tarmoqlar va messenjerlarda zararli ilovalar hamda xavfli havolalarni tarqatish orqali sodir etilishi mumkin bo‘lgan kiberjinoyatlarning oldini olishga qaratilgan avtomatlashtirilgan profilaktik mexanizmni ilmiy jihatdan asoslash va amaliyotda qo‘llanilayotgan Telegram bot yechimining imkoniyatlarini tahlil qilishdan iborat.

Ushbu maqsadga erishish uchun quyidagi vazifalar belgilandi: zararli mobil ilovalar va xavfli havolalar orqali sodir etiladigan kiberxavflarni tahlil qilish; Telegram muhitida avtomatik profilaktika mexanizmlarini o‘rganish; zararli kontentni aniqlash va o‘chirishga mo‘ljallangan botning funksional vazifalarini belgilash; botning

amaliyotda qo‘llanilishi natijasida yuzaga keladigan profilaktik samarani baholash; tizimni takomillashtirish bo‘yicha ilmiy-amaliy takliflar ishlab chiqish.

**Zararli ilovalar va havolalar orqali kiberxavflarning shakllanishi**

Zararli mobil ilova — foydalanuvchining qurilmasiga o‘rnatilganidan so‘ng uning ma’lumotlari, hisob ma’lumotlari yoki qurilma funksiyalaridan noqonuniy foydalanishga olib kelishi mumkin bo‘lgan dasturiy vosita sifatida qaraladi. Bunday ilovalar turli shakllarda tarqatilishi mumkin: APK fayllari, soxta dasturlar, modifikatsiya qilingan ilovalar, fishing sahifalariga olib boruvchi havolalar va boshqalar.

Muammoning xavfli jihati shundaki, zararli kontentning dastlabki tarqalish bosqichida foydalanuvchi ko‘pincha uning haqiqiy maqsadini anglamaydi. Masalan, xabarda bank ilovasining yangilangan versiyasi, elektron hujjat, to‘lov tasdig‘i yoki boshqa xizmatga oid fayl sifatida ko‘rsatilgan zararli ilova tarqatilishi mumkin. Agar foydalanuvchi faylni o‘rnatsa yoki havolaga o‘tsa, keyingi bosqichda shaxsiy va moliyaviy ma’lumotlarning buzilishi yoki qo‘lga kiritilishi xavfi ortadi.

Shu sababli kiberjinoyatlarning oldini olish faqat zararli dastur qurilmaga o‘rnatilgandan keyin uni aniqlash bilan cheklanmasligi lozim. Profilaktikaning samarali modeli zararli kontentni potensial jabrlanuvchiga yetib borishidan oldin aniqlash va uni tarqatish kanalidan olib tashlash tamoyiliga asoslanishi mumkin.

**Ishlab chiqilgan Telegram botning funksional imkoniyatlari**

Tadqiqotning amaliy qismi doirasida Telegram platformasi uchun @samcyber_102bot manzilida avtomatlashtirilgan bot ishlab chiqilgan. Bot Telegram kanallari va guruhlarida tarqatilayotgan xabarlarni belgilangan qoidalar asosida tahlil qilish, zararli yoki shubhali kontentni aniqlash va zarur hollarda xabarni avtomatik ravishda o‘chirishga qaratilgan.

Texnik nuqtayi nazardan, Telegram Bot API botlarga xabarlar bilan ishlash va tegishli huquqlar mavjud bo‘lganda guruh yoki kanallardagi xabarlarni o‘chirish imkonini beradi. Telegram hujjatlarida xabarni o‘chirish uchun botga tegishli ma’muriy huquqlar berilishi zarurligi ko‘rsatilgan. Shuningdek, xabarni o‘chirish bo‘yicha texnik cheklovlar mavjud [3].

Botning umumiy ishlash algoritmini quyidagi bosqichlarga ajratish mumkin: 1) Telegram guruhi yoki kanalida yangi xabar paydo bo‘lishi; 2) xabar matni, havolasi yoki fayl turining dastlabki tahlili; 3) zararli kontentga xos belgilarni aniqlash; 4) belgilangan xavf mezonlari bo‘yicha qaror qabul qilish; 5) xavfli deb baholangan xabarni avtomatik o‘chirish; 6) zaruratga ko‘ra administrator yoki foydalanuvchini ogohlantirish; 7) tizim statistikasi uchun texnik jurnal ma’lumotlarini shakllantirish.

Bunday arxitekturaning asosiy afzalligi — profilaktik ta’sirning tezkorligidadir. Agar zararli xabar tarqalganidan keyin qisqa vaqt ichida aniqlanib, o‘chirilsa, uni ko‘rish, faylni yuklab olish yoki havolaga o‘tish ehtimoli pasayadi. Demak, avtomatik moderatsiya mexanizmi kiberhujumning foydalanuvchi qurilmasigacha bo‘lgan zanjirida profilaktik to‘siq vazifasini bajaradi.

**Amaliy natijalar va joriy etilganlik**

Tadqiqotning muhim amaliy natijasi ishlab chiqilgan botning faqat tajriba tariqasida emas, balki amaliyotda qo‘llanilayotganligi bilan izohlanadi. Mavjud ma’lumotlarga ko‘ra, botdan hozirgi vaqtda 30 000 dan ortiq Telegram guruhlari va kanallarida foydalanib kelinmoqda. Ushbu ko‘rsatkich yechimning keng qamrovda qo‘llanilayotganini va uning amaliy ahamiyatini ko‘rsatuvchi muhim mezon hisoblanadi.

Botning keng qamrovda qo‘llanilishi natijasida Telegram muhitida zararli ilovalar va xavfli havolalarning tarqalishini tezkor cheklash imkoniyati paydo bo‘ladi. Bu mexanizm foydalanuvchining zararli faylni ochishi, zararli ilovani o‘rnatishi yoki fishing resursiga kirib, maxfiy ma’lumotlarni taqdim etishi ehtimolini kamaytirishga xizmat qiladi.

Profilaktik nuqtayi nazardan, bunday tizimning ahamiyati shundaki, u kiberjinoyat oqibatlarini bartaraf etishdan ko‘ra, jinoyatga olib kelishi mumkin bo‘lgan kontentni tarqatish bosqichiga ta’sir ko‘rsatadi. Xususan, bank kartalari va boshqa moliyaviy hisobvaraqlardan mablag‘larni noqonuniy ravishda yechib olish yoki o‘tkazishga olib kelishi mumkin bo‘lgan zararli dasturlar tarqalishini cheklash, shuningdek, shaxsiy ma’lumotlar va akkaunt rekvizitlarining kiberjinoyatchilar qo‘liga tushib qolish xavfini kamaytirishga xizmat qiladi.

Shu bilan birga, mazkur natijalarni ilmiy jihatdan baholashda ehtiyotkorlik talab etiladi. Botning mavjudligi kiberjinoyatlarni mutlaq ravishda bartaraf etadi, degan xulosaga olib kelmasligi kerak. Uning samaradorligi zararli kontentni aniqlash mezonlarining sifatiga, yangi tahdidlar haqidagi ma’lumotlarni muntazam yangilashga, Telegram API imkoniyatlariga va guruh hamda kanal administratorlari tomonidan berilgan huquqlarga bog‘liq.

**Ayollar va bolalarga nisbatan zo‘ravonlikning raqamli muhitdagi ko‘rinishlari**

Raqamli kommunikatsiya vositalarining kengayishi zo‘ravonlikning ayrim shakllarini onlayn muhitga ko‘chirish yoki ularni texnologiyalar yordamida kuchaytirish imkonini ham yaratadi. Ayollar va bolalarga nisbatan kiberzo‘ravonlik tushunchasi doirasida tahdidli xabarlar yuborish, muntazam ravishda ta’qib qilish, soxta akkauntlar orqali bosim o‘tkazish, shaxsiy ma’lumotlarni roziliksiz tarqatish, haqorat yoki shantaj qilish, zararli havolalar va fayllar yordamida qurilmaga yoki akkauntga kirishga urinish kabi holatlar ko‘rib chiqilishi mumkin. Bunday harakatlar real hayotdagi zo‘ravonlik bilan bog‘liq bo‘lishi yoki mustaqil raqamli tajovuz sifatida namoyon bo‘lishi mumkin.

**Muammoning kriminologik omillari**

Ayollar va bolalarga nisbatan raqamli zo‘ravonlikni kriminologik jihatdan tahlil qilishda bir nechta omillarni hisobga olish zarur. Birinchidan, anonimlik yoki soxta akkauntlardan foydalanish tajovuzkorning o‘zini yashirishiga imkon berishi mumkin. Ikkinchidan, ijtimoiy tarmoqlarda kontentning tez tarqalishi bir martalik tahdid yoki haqoratning katta auditoriyaga yetib borishiga sabab bo‘ladi. Uchinchidan, jabrlanuvchining raqamli xavfsizlik bo‘yicha bilimlari yetarli bo‘lmasa, fishing yoki zararli ilova orqali akkauntni egallash xavfi ortadi. Bolalar uchun esa yoshga mos bo‘lmagan kontent, begona shaxslar bilan muloqot va raqamli bosim alohida profilaktik yondashuvni talab qiladi.

**Zararli ilovalar va kiberzo‘ravonlik o‘rtasidagi bog‘liqlik**

Zararli ilovalar va havolalar faqat moliyaviy zarar yetkazish vositasi bo‘lib qolmay, jabrlanuvchini kuzatish, akkauntlarga noqonuniy kirish yoki shaxsiy

ma’lumotlarni qo‘lga kiritish uchun ham ishlatilishi mumkin. Shu sababli ayollar va bolalarga qarshi kiberzo‘ravonlikning oldini olishda zararli kontentni texnik jihatdan aniqlash bilan bir qatorda, uning kimga va qanday vaziyatda yo‘naltirilayotganini ham hisobga oladigan profilaktik model zarur. Bunda foydalanuvchining shaxsiy hayoti va qonuniy huquqlariga rioya qilish, ortiqcha monitoringga yo‘l qo‘ymaslik ham muhim hisoblanadi.

**Innovatsion yechimlar**

Innovatsion profilaktika vositasi sifatida zararli kontentni avtomatik aniqlash, xavf indikatorlarini muntazam yangilash, anonimlashtirilgan statistik tahlil va inson nazoratini birlashtiruvchi gibrid model taklif etiladi. Bunday modelda avtomatik tizim dastlabki xavfni aniqlaydi, murakkab yoki noaniq holatlarda esa moderator yoki vakolatli administrator tomonidan qayta ko‘rib chiqish imkoniyati saqlanadi. Ayniqsa, bolalar bilan bog‘liq holatlarda xavf darajasini baholash, tezkor ogohlantirish va dalillarni qonuniy tartibda saqlash mexanizmlari alohida ahamiyatga ega.

**Ayollar va bolalarni himoya qilishda @samcyber_102bot imkoniyatlaridan foydalanish**

Tadqiqot doirasida ishlab chiqilgan @samcyber_102botning zararli ilovalar va havolalarni aniqlash hamda o‘chirishga qaratilgan funksiyalari ayollar va bolalar ishtirok etadigan onlayn muhitda qo‘shimcha profilaktik qatlam sifatida qo‘llanishi mumkin. Bunda botning vazifasi shaxslarni kuzatish emas, balki xavfli kontentning tarqalish zanjirini uzishga qaratilishi lozim. Mazkur yondashuv shaxsiy hayot daxlsizligi, ma’lumotlarni minimallashtirish va qonuniy asosda ishlash tamoyillari bilan uyg‘unlashtirilishi kerak. Botning amaliyotda 30 000 dan ortiq Telegram guruhlari va kanallarida qo‘llanilayotgani haqidagi mavjud ma’lumot ushbu profilaktik vositaning keng ko‘lamda qo‘llanishini ko‘rsatadi; biroq bu ko‘rsatkichning o‘zi zo‘ravonlik holatlari kamayganini statistik jihatdan isbotlamaydi.

**Takomillashtirish yo‘nalishlari**

Birinchi navbatda, zararli havolalarni aniqlashda domen va URL reputatsiyasi, havolaning yo‘nalishi, domenning yaratilish xususiyatlari, shubhali yo‘naltirishlar va boshqa texnik belgilardan foydalanish mumkin. Biroq avtomatik qaror qabul qilishda

noto‘g‘ri ijobiy natijalarni kamaytirish muhim. Aks holda qonuniy xabarlar ham asossiz ravishda o‘chirilishi mumkin.

Ikkinchi yo‘nalish — zararli fayllarni, xususan, APK fayllarini ko‘p bosqichli tahlil qilish. Fayl kengaytmasi, nomi yoki matndagi kalit so‘zning o‘zi yetarli mezon bo‘lmasligi mumkin. Shuning uchun faylning kriptografik xesh qiymati, ma’lum zararli fayllar bazasi, raqamli imzo xususiyatlari va xavf indikatorlaridan kompleks foydalanish maqsadga muvofiq.

Uchinchi yo‘nalish — statistik va mashinali tahlil usullarini joriy etish. Bot orqali aniqlangan zararli xabarlar bo‘yicha anonimlashtirilgan statistika shakllantirilib, qaysi turdagi fayllar, havolalar va tarqatish usullari ko‘proq uchrayotganini tahlil qilish mumkin. Bu ma’lumotlar profilaktika choralarini takomillashtirish va yangi tahdidlarni oldindan aniqlash uchun xizmat qilishi mumkin.

To‘rtinchi yo‘nalish — inson omilini hisobga olish. Har qanday avtomatik tizim xatolarga duch kelishi mumkinligi sababli murakkab yoki yuqori xavfli holatlarda administratorga xabar berish, qarorni qayta ko‘rib chiqish imkonini saqlash maqsadga muvofiq. Shu tariqa avtomatlashtirish va inson nazorati o‘rtasidagi muvozanat ta’minlanadi.

**Xulosa**

Ijtimoiy tarmoqlar va messenjerlar orqali zararli ilovalar hamda xavfli havolalarni tarqatish zamonaviy kiberjinoyatlarni sodir etishda muhim vositalardan biri bo‘lib qolmoqda. Bunday kontentdan foydalanish orqali foydalanuvchilarning shaxsiy ma’lumotlari, akkauntlari va moliyaviy resurslariga tahdid yuzaga kelishi mumkin.

Tadqiqot doirasida ishlab chiqilgan @samcyber_102bot ushbu muammoning profilaktik yechimi sifatida Telegram kanallari va guruhlarida zararli kontentni avtomatik aniqlash va o‘chirishga qaratilgan. Botning amaliyotda qo‘llanilayotgani va 30 000 dan ortiq guruh hamda kanallarda foydalanilayotgani uning amaliy ahamiyatini ko‘rsatadi.

Ushbu yechim zararli ilovalarning foydalanuvchi qurilmasiga o‘rnatilishi va xavfli havolalar orqali fishing resurslariga kirish ehtimolini kamaytirishga xizmat

qilishi mumkin. Shu orqali fuqarolarning bank kartalari va boshqa moliyaviy hisoblaridagi mablag‘larni noqonuniy o‘zlashtirish, shuningdek, shaxsiy va maxfiy ma’lumotlarning kiberjinoyatchilar qo‘liga tushib qolish xavfini pasaytirishga qaratilgan profilaktik mexanizm yaratiladi.

Kelgusida tizimni zararli URL va fayllarni chuqurroq tahlil qilish, tahdid indikatorlari bazasini muntazam yangilash, mashinali tahlil usullarini joriy etish, statistik monitoringni kuchaytirish va inson nazorati bilan uyg‘unlashtirish maqsadga muvofiq. Bunday yondashuv ijtimoiy tarmoqlar orqali sodir etilayotgan kiberjinoyatlarning oldini olish samaradorligini oshirishga xizmat qilishi mumkin.

**Foydalanilgan adabiyotlar**

1. Souppaya M., Howell G., Scarfone K., Franklin J., Sritapan V. Guidelines for Managing the Security of Mobile Devices in the Enterprise. NIST Special Publication 800-124 Rev. 2. National Institute of Standards and Technology, 2023.

2. Howell G., Boeckl K., Grayson N., Lefkovitz N., Ajmo J., Craft R. E., McGinnis M., Sandlin K., Slivina O., Snyder J., Ward P. Mobile Device Security: Bring Your Own Device (BYOD). NIST Special Publication 1800-22. National Institute of Standards and Technology, 2023.

3. Telegram. Telegram Bot API Documentation. Telegram Messenger LLP. Bot API methods, including message deletion and administrator permissions. https://core.telegram.org/bots/api

4. National Institute of Standards and Technology (NIST). Mobile Threat Catalogue. Mobile device threat taxonomy and threat descriptions. https://pages.nist.gov/mobile-threat-catalogue/

5. NIST. Digital Identity Guidelines: Authentication and Lifecycle Management. NIST Special Publication 800-63B. National Institute of Standards and Technology.

6. UN Women. Frequently asked questions: Types of violence against women and girls, including technology-facilitated violence.

7. UNICEF. Child online safety: guidance and resources on protecting children in digital environments.

8. Council of Europe. Protection of children against sexual exploitation and sexual abuse in the digital environment.