IJTIMOIY TARMOQLARDA DESTRUKTIV AXBOROTLARNING TARQALISHINI MATEMATIK MODELLASHTIRISH (SI, SIR, SIRS MODELLARI ASOSIDA)

Abdazimov Saidaminxo‘dja Zoirxo‘dja o‘g‘li
IIV Akademiyasi Raqamli texnologiyalar va Axborot xavfsizligi kafedrasi,o‘qituvchisi

https://doi.org/10.5281/zenodo.15522459

Annotatsiya. *Ushbu maqolada ijtimjoiy tarmoqlarda axborot xurujlarini tarqalish ehtimolligini bashoratlash va ulardan himoyalash usuli va modellarini takomillashtirishga bag‘ishlangan. Ijtimoiy tarmoqlarda buzg‘unchi ma‘lumotlarni tarqatish mexanizmiga qarab axborot xurujlarining tarqalish darajasi bo‘yicha ehtimoliy taxminlarni olishga imkon beruvchi matematik modellar takomillashtirilgan.*

Kalit so‘zlar: *axborot xavfsizligi, kiberxujum, kiberjinoyatchi, ijtimoiy tarmoqlarning arxitekturasi.*

Аннотация. *Данная статья посвящена совершенствованию методов и моделей прогнозирования и защиты от распространения информационных атак в социальных сетях. Усовершенствованные математические модели, позволяющие получать вероятные оценки распространенности информационных атак в зависимости от механизма распространения подрывной информации в социальных сетях***.**

Ключевые слова*: информационная безопасность, кибератака, киберпреступник, архитектура социальной сети.*

Annotation. *This article is devoted to the improvement of methods and models for predicting and protecting against the spread of information attacks in social networks. Improved mathematical models that make it possible to obtain probable estimates of the prevalence of information attacks, depending on the mechanism of dissemination of subversive information in social networks.*

Keywords: *information security, cyberattack, cybercriminal, social network architecture.*

Axborot texnologiyalarini rivojlantirish va ularni jamiyat faoliyatining barcha sohalarida amalga oshirish axborot xavfsizligi tizimlarini joriy etishni o‘z ichiga oladi. Buning sababi zamonaviy texnologiyalar paydo bo‘lishi bilan turli xil tahdidlar virtual muhitda jadal rivojlanmoqda, va mavjud axborot xavfsizligi texnologiyalari eskirmoqda. So‘nggi bir necha yil ichida bu hodisa ancha sezilarli bo‘lib qoldi. “Kiberjinoyatchining asosiy istagi tahdidlar amalga oshirilishidan foyda olish va texnologiya qancha ko‘p imkoniyatlar yaratsa, ular (kiberjinoyatchilar) o‘z niyatlarini amalga oshirishda shuncha ko‘p imkoniyatlarga ega bo‘lishadi” So‘nggi yillarda O‘zbekiston Respublikasida axborot xavfsizligi quyidagi yo‘nalishlarda amalga oshirilmoqda.

Bu:

1. Normativ-huquqiy bazani takomillashtirish va rivojlantirish.
2. Axborot xavfsizligini ta‘minlash dasturiy ta‘minotini ishlab chiqish va amalga oshirish.

Xalqaro ta‘sir o‘tkazish va boshqa mamlakatlar bilan ilg‘or tajribalarni almashish. Yuqorida aytib o‘tilganlarga qaramay, axborot xavfsizligi sohasida zarur choralarni ishlab chiqish va muvofiqlashtirish masalalari haligacha dolzarb bo‘lib turibdi[1-2].

Axborot va psixologik xavfsizlik davlat, jamiyat va xususiy shaxs tomonidan amalga oshiriladigan, har qanday joyda axborot texnologiyalariga hamroh bo‘ladigan, ular bilan bir joyda to‘liq birlashish darajasigacha bo‘lgan jarayonlar va choralardir.

Kiberhujumlik psixologik zarar etkazishga qaratilgan hujumlar bo‘lib, ular turli xil aloqa

platformalari: elektron pochta, tezkor xabar almashish xizmatlari, suhbat xonalari, ijtimoiy tarmoqlar, veb-saytlar, shuningdek, mobil aloqa va Internet orqali amalga oshiriladi.

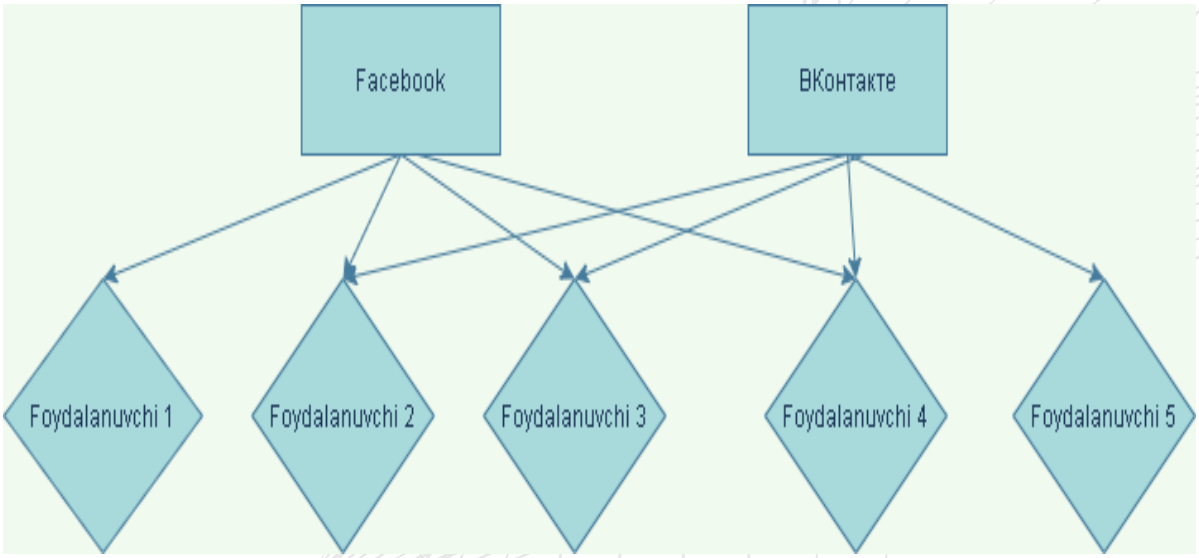
Agar xodimlar tarkibida axborot xavfsizligi bo‘yicha yaxshi mutaxassislarga ega bo‘lgan tashkilotlar biron bir himoyaga ega bo‘lsa, unda ma‘lumotlar uzatish tarmoqlarining oddiy foydalanuvchisi xavfsizlik jarayonidagi eng himoyalanmagan bo‘g‘in hisoblanadi.

Ko‘pincha ular trolling, kashchenizm yoki kiberhujumlarning turli xil turlari qurbonlari bo‘ladi. Afsuski, maxsus ma‘lumotga ega bo‘lmagan yoki biron bir kompyuter mahoratiga ega bo‘lmagan oddiy foydalanuvchi Internet axborot xavfsizligi tahdidlarining himoyasiz qurboniga aylanadi. Shuning uchun ular ko‘pincha kiberjinoyatchilarning qurboniga aylanishlari ajablanarli emas. Hujum tashkilotga qaratilgan bo‘lsa ham, foydalanuvchi baribir qurbon bo‘ladi.

Axborot-kommunikatsiya tizimlarida ijtimoiy tarmoqlar tuzilishini tahlil qilish

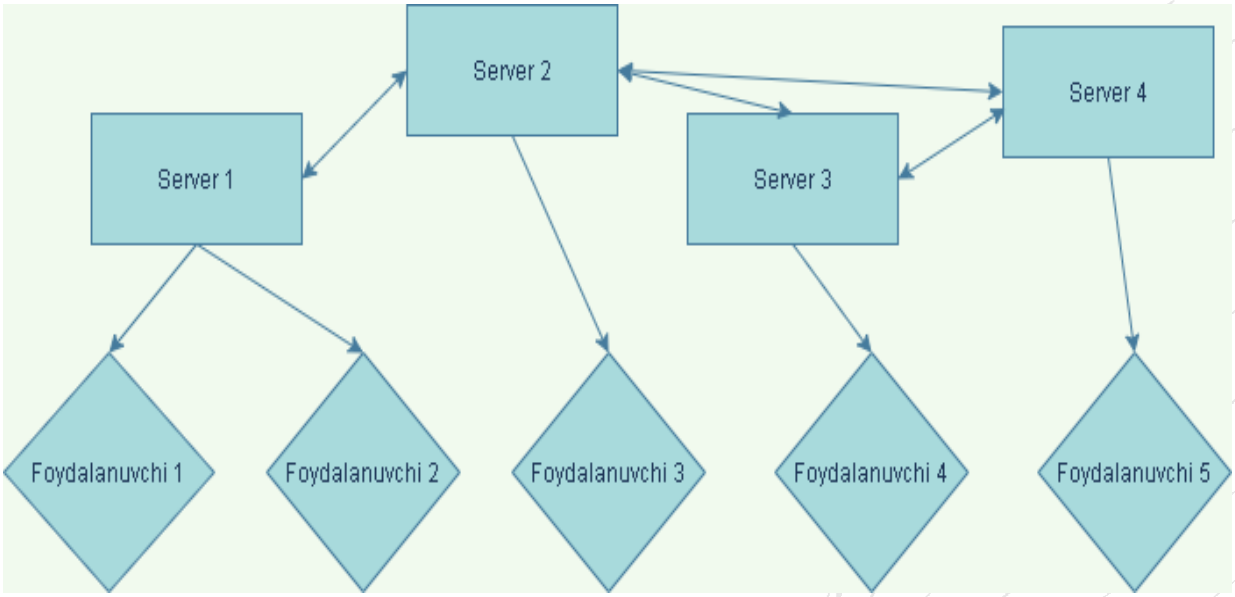
Ijtimoiy tarmoq deganda $G = (V, E)$ grafigi sifatida aks ettirilishi mumkin bo‘lgan tugunlar to‘plami (foydalanuvchilar, guruhlar yoki jamoalar) va ular orasidagi bog‘lanishlar (ijtimoiy o‘zaro aloqalar) dan iborat bo‘lgan tuzilma tushuniladi.

Ijtimoiy tarmoqlarni arxitekturasi bo‘yicha quyidagi guruhlarga bo‘lish mumkin:



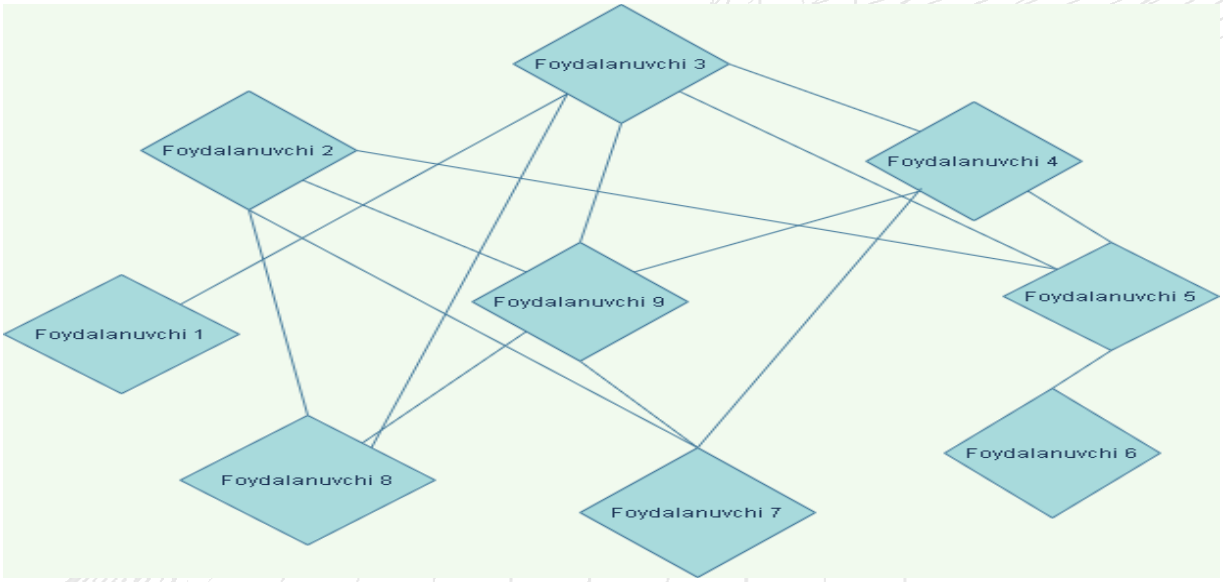
1.1.-rasm. Ijtimoiy tarmoqlarning markazlashtirilgan arxitekturasi

Qisman markazlashtirilmagan (gibrid) yechimlar (1.2-rasm). Birgina misol bu ko‘plab o‘zaro bog‘langan tugunlardan tashkil topgan *Diaspora* ijtimoiy tarmog‘i, ularning har biri alohida veb-server. Ijtimoiy tarmoq mijoz-server arxitekturasiga ega, foydalanuvchilar ulanadigan serverni tanlashlari mumkin.



1.2-rasm. Qisman markazlashtirilmagan ijtimoiy tarmoq arxitekturasi

To‘liq markazlashtirilmagan P2P (peer-to-peer) ijtimoiy tarmoqlari (1.3-rasm). Ma‘lumotlar mijoz tomonidan saqlanadi va qayta ishlanadi [3-4], bu ham serverdir. Ushbu ijtimoiy tarmoqlarga quyidagilar kiradi: *LifeSocial*, *PeerSoN*, *Safebook*, *Pandora*.



1.3-rasm. To‘liq markazlashtirilmagan ijtimoiy tarmoq arxitekturasi

Shunday qilib, biz xulosaga kelishimiz mumkinki, agar ijtimoiy tarmoqlarda buzg‘unchi ma‘lumotlarning tarqalishini to‘xtatish zarur bo‘lsa, foydalanuvchilarning butun ijtimoiy tarmoqni to‘liq blokirovka qilish kerak bo‘lmasdan tarqalishi va o‘zaro aloqasi amalga oshiriladigan bir nechta tugunlarni blokirovka qilish kifoya.

Ijtimoiy tarmoqlarda axborot xurujlari turlarining xususiyatlari

Axborot tahdidi - bu axborot xavfsizligi buzilishining potentsial yoki real tahdidini vujudga keltiradigan shart-sharoitlar va omillar majmuidir.

Axborot xurujlariga qarshi tarqalishi va qurish himoya qismlarining oldindan ularning

tasnifi xususiyatlarni ta‘kidlash lozim bo‘ladi.

Ijtimoiy tarmoqlardagi axborot xurujlari bir necha asosiy mezonlarga muvofiq tasniflanishi mumkin:

- *ta‘sir etish ob‘ektlari;*
- *ta‘sir maqsadi;*
- *xurujlarni amalga oshirish usullari;*
- *ta‘sir qilish manbalari;*

Ta‘sir ob‘ektlari:

- Ijtimoiy tarmoq foydalanuvchilari;
- Ishlab chiquvchilar, ma‘muriyat va texnik xodimlar;
- Uskuna (serverlar, ish stantsiyalari, tarmoq uskunalari, aloqa kanallari);
- Dasturiy ta‘minot.

Ta‘sir maqsadlari:

Texnik va axborot (dasturiy ta‘minotga ta‘sir):

- uskunalari bilan ishlashning buzulishi;
- aloqa kanalining mavjudligini cheklash;
- Ma‘lumotlarning yaxlitligi va dolzarbligini buzish. Ma‘lumotni o‘zgartirish yoki olib tashlash;

Axborot tahdidlarga almashish taxmin asoslangan usullari izomorfizma qo‘yish mumkin. Ba‘zi biologik modellar ijtimoiy tarmoqlarda qo‘llanilishi uchun moslashtirilishi mumkin.

Buzg‘unchi ma‘lumotlarni tarqatish jarayonini tavsiflashda biologik yondashuvlardan foydalanadigan matematik modellar differentsial tenglamalar va epidemik jarayonni bir nechta diskret holatlardan birida ob‘ektlar sonining o‘zgarishi sifatida aks ettirishga asoslangan.

Axborot xurujlarini SI matematik modeli asosida taqsimlash (Susceptible-Infected)

Misollardan birida SI *(Susceptible-Infected)* matematik modeli, u ob‘ektlarning ikkita holatining mavjudligi bilan tavsiflanadi: yuqtirilgan (I) va yuqtirilmagan (S).

SI modeliga asoslangan ijtimoiy tarmoqning umumiy tuzilishi bo‘lishi mumkin:

$$N = S(t) + I(t)$$

bu erda:

N —ijtimoiy tarmoqdagi foydalanuvchilarning umumiy soni;

$S(t)$ — buzg‘unchi ma‘lumotlar bilan tanish bo‘lmagan foydalanuvchilar soni;

(t) — buzg‘unchi ma‘lumotni ijobiy qabul qilgan va uning ijtimoiy tarmoqda tarqalishiga hissa qo‘shgan foydalanuvchilar soni.

Shubhasiz, ushbu model ilgari $S(t)$ buzg‘unchi ma‘lumotlari bilan tanish bo‘lmagan foydalanuvchilarning ma‘lum bir qismi destruktiv ma‘lumotlarga qarshi immunitetga ega bo‘lib chiqishini hisobga olmaydi. Bunday holda, foydalanuvchi mmunitetini hisobga olgan holda, SI modeli *SIR (SI-Recovered)* modeliga aylantiriladi.

SIR (Susceptible-Infected-Recovered) matematik modeli asosida axborot xurujlarini taqsimlash

SIR (Susceptible-Infected-Recovered) matematik modeli uch xil ob‘ekt holatiga ega: yuqtirilmagan (S), yuqtirilgan (I) va immuniteti (R) bo‘lgan dezinfektsiyalangan ob‘ektlar.

SIR modeliga asoslangan ijtimoiy tarmoqning umumiy tuzilishi quidagicha bo‘lishi mumkin:

$N = S(t) + I(t) + R(t)$ ifodasi yordamida ifodalangan.

bu erda:

N – ijtimoiy tarmoqdagi foydalanuvchilar umumiy soni;

$S(t)$ – buzg‘unchi ma‘lumotlar bilan tanish bo‘lmagan foydalanuvchilar soni;

$I(t)$ – buzg‘unchi ma‘lumotni ijobiy qabul qilgan va uning ijtimoiy tarmoqda tarqalishiga hissa qo‘shgan foydalanuvchilar soni;

$R(t)$ – bu bo‘lmagan foydalanuvchilar soni.

Agar harakat (xabar berish) bir lahzada sodir bo‘lsa, bayonot to‘g‘ri, ammo agar ma‘lum bir vaqt ichida sodir bo‘lsa, unda yangi foydalanuvchilar tufayli N sonining ko‘payishi va masalan, N ning kamayishi, hisoblarni blokirovka qilish yoki o‘chirish kuzatiladi.

Matematik model va SIRS (Susceptible-Infected-Recovered-Susceptible) asosida axborot xurujlarini tarqatish

SIR modelining kamchiliklaridan biri shundaki, ilgari javob bermaydigan foydalanuvchilar kelajakda buzg‘unchi ma‘lumotlarga ta‘sir etishi mumkin. Ushbu kamchilik *SIR* modelini *SIRS (sezgir-yuqtirgan-tiklanadigan-sezgir)* modeliga aylantirish orqali yo‘q qilinadi, bunda ilgari javob bermaydigan foydalanuvchi bir muncha vaqt o‘tgach sezgir bo‘lib qoladi. Boshqaruv ob‘ektining qo‘shimcha turini joriy etish va yangi mumkin bo‘lgan diskret holatlarni hisobga olish ham matematik modelning aniqligini oshirishga imkon beradi, ammo real sharoitlarda bir holatdan boshqasiga va orqaga o‘tishni kafolatlab bo‘lmaydi. Shuni yodda tutish kerakki, axborot urushi vositalari darhol ishlay olmaydi, lekin faqat ma‘lum bir vaqtdan keyin ishga tushishi mumkin [5]. Kuchli axborot qarama-qarshiliklari sharoitida foydalanuvchi bir necha marta bir holatdan ikkinchisiga o‘tishi mumkin yoki destruktiv ma‘lumotlarga umuman ahamiyat bermaydi. Ushbu omillar *SIRS* modelida hisobga olinmaydi, bu esa ushbu model doirasini qisqartiradi. Ushbu modelning afzalligi bu tatbiq etishning soddaligi, ammo real sharoitda ushbu modelni qo‘llash axborotga salbiy ta‘sir ko‘rsatish bosqichida cheklangan.

Xulosa

Xulosa qilish mumkinki, axborot tahdidlarining tarqalishini tavsiflovchi matematik modellarda biologik yondashuvlardan foydalanish xarakterli xususiyatlarni aniqlashga va tarqalishning matematik bahosini olishga imkon beradi. SIR modeli eng aniq tasvirlangan buzg‘unchi ma‘lumotlarni tarqatish jarayoni va ayrim hollarda axborot tahdidlarining tarqalishini bashorat qilish uchun ishlatilishi mumkin.

REFERENCES

1. Акулич, М.М. (2012) Троллинг в социальных сетях: возникновение и развитие. Электронный ресурс. // journals.rudn.ru › sociology › article.
2. Курилкин, А. В. (2019) Проблемы информационно- психологического манипулирования в пространстве сети Facebook. Электронный ресурс.
3. Котенко И.В., Воронцов В.В. Аналитические модели распространения сетевых червей // Труды СПИИРАН. 2007. Вып. 4. С. 208-224.
4. Д.А. Губанов, Д.А. Новиков, А.Г. Чхартишвили, Модели информационного влияния и информационного управления в социальных сетях // Проблемы управления, 2009, № 5, С. 28–35
5. Savchenko I.I., Gatcenko O.I. Analytical review of methods of providing internet anonymity // Automatic Control and Computer Sciences - 2015, Vol. 49, No. 8, P. 696-700