

## FEYK MA'LUMOTLAR QANDAY TARQALADI? BOTLAR, ODAMLAR, TROLLAR VA MIKROTARGETING

O'zDJTU magistranti

Abdurahmonov Zayniddin

**Annotatsiya:** *Ushbu maqolada biz botlar va oddiy odamlar soxta xabarlarini qanday tarqatishini; odamlarning veb-saytlarga tashrifini qayd qilishda cookie-fayllardan qanday foydalanishini, shaxsiy profillarni yaratishni o'rganamiz va ularga eng ko'p qabul qiladigan soxta yangiliklar kontentini ko'rsatamiz. Shuningdek, biz trollarni, ya'ni yolg'on xabar tarqatish va noto'g'ri ma'lumotlarni avj oldirish uchun ijtimoiy tarmoqlarda akkaunt ochgan odamlarni ham ko'rib chiqamiz.*

**Kalit so'zlar:** *Botlar, trolling, mikrotargeting, cookie-fayllar, ijtimoiy media platformalari, soxta yangiliklar, heshteg, noto'g'ri ma'lumotlar*

**Annotation:** *In this article, we will learn how bots and ordinary people spread fake news; how people use cookies when recording visits to websites, how to create personal profiles, and show them Fake News content that they receive the most. We will also look at trolls, that is, people who have opened an account on social networks to spread false news and escalate misinformation.*

**Keywords:** *Bots, trolling, microtargeting, Cookies, social media platforms, fake news, hashtag, misinformation*

**Аннотация:** *В этой статье мы узнаем, как боты и обычные люди распространяют поддельные сообщения; как люди используют файлы cookie для записи своих посещений веб-сайтов, как создавать личные профили и показывать им поддельный новостной контент, который они получают больше всего. Мы также рассмотрим троллей, то есть людей, которые создали учетные записи в социальных сетях для распространения ложных новостей и распространения дезинформации.*

**Ключевые слова:** *боты, троллинг, микротаргетинг, файлы cookie, платформы социальных сетей, поддельные новости, хэштеги, дезинформация*

## KIRISH

**Botlar va feyk yangiliklarni targ'ib qilish.** Ijtimoiy tarmoqlardan foydalanadigan milliardlab odamlardan tashqari, millionlab robotlar yoki botlar ham mavjud. Botlar soxta yangiliklarni tarqatishga yordam beradi va ijtimoiy tarmoqlarda soxta yangiliklarning mashhurligini oshiradi. Ijtimoiy media platformalari (Facebook, Twitter, Instagram va boshqalar) soxta yangiliklar tarqatuvchi millionlab ijtimoiy botlarning xonadoniga aylandi. 2017-yilgi hisob-kitoblarga ko'ra, Twitterda 23 million bot (barcha akkauntlarning 8,5 foizi), Facebookda 140 million bot (akkauntlarning 5,5 foizigacha) va Instagramda 27 millionga yaqin bot (akkauntlarning 8,2 foizi) mavjud [1]. Bu ijtimoiy tarmoqlardagi 190 million bot - butun AQShda yashovchi odamlar sonining yarmidan ko'pi! Botlar “Yulduzli urushi” filmidagi R2D2 kabi jismoniy shaxslar emas. Ular kompyuter dasturlash qobiliyatiga ega bo'lgan odamlar tomonidan yaratilgan va ijtimoiy media platformalarida istiqomat qiladi, ular faqat koddan, ya'ni kompyuter ko'rsatmalaridan iborat. Shunday qilib, botlar - bu vazifalarni avtonom va takroriy bajarish uchun onlayn ijtimoiy tarmoq saytlarida ishlaydigan kompyuter algoritmlari (ma'lum bir vazifani bajarish uchun mantiqiy qadamlar to'plami). Ular ijtimoiy tarmoqdagi odamlarning xatti-harakatlariga taqlid qiladi, boshqa foydalanuvchilar bilan muloqot qiladi, ma'lumot va xabarlarni almashadi [1]–[3]. Mantiqiy algoritmlar tufayli botlar muayyan vaziyatlarga qanday reaksiya berishni o'rganishlari mumkin. Ya'ni, ular sun'iy intellektga ega.

## ADABIYOTLAR SHARHI VA METODLAR

Sun'iy intellekt botlarga internet foydalanuvchilarining xatti-harakatlariga taqlid qilish imkonini beradi (masalan, ijtimoiy tarmoqlarda qoldirilgan fikr namunalariga o'xshab), bu soxta yangiliklarni tarqatishda yordam beradi. Misol uchun, Twitterda botlar ularni oddiy odamlardek ko'rsatadigan ijtimoiy munosabatlarga taqlid qilishi mumkin. Ular nufuzli Twitter foydalanuvchilarini (ko'p obunachilari bo'lgan Twitter foydalanuvchilarini) qidiradilar va ularga e'tibor berish va almashishni ko'rgan boshqa Twitter foydalanuvchilarida ishonch hosil qilish uchun ularga savollar yuborish orqali bog'lanadilar. Ular foydalanish uchun dasturlashtirilgan skriptlar asosida boshqalarning xabarlari yoki savollariga javob berishadi. Ular, shuningdek, ommabop mavzular haqida xabarlar joylashtirish orqali bahs-munozaralarni keltirib chiqaradi - Twitter har doim foydalanuvchilarga nima trend bo'layotganini ko'rsatadi, boshqa veb-saytlarda topilgan mavzuga oid ma'lumotlarni qidirish va takrorlash orqali buni amalga oshiradi [4].

## TAHLIL VA NATIJALAR

**Botlar soxta yangiliklarni tarqatishda qanday yordam beradi?** Botlar soxta yangiliklarni, birinchi navbatda, internetda tekshirilmagan ma'lumotni (hali tasdiqlanmagan ma'lumotni) qidirish va olish orqali tarqatadi. Ikkinchidan, botlar kengroq auditoriyani qamrab olishning asosiy strategiyasi sifatida ommabop mavzular va heshteglardan foydalangan holda, ko'p hollarda soxta yangiliklarning tarqalishiga yordam beradigan asosiy strategiya sifatida tanlanmagan kontentni ijtimoiy media saytlarida doimiy ravishda joylashtiradi. Shunday qilib, botlar soxta yangiliklarni ikki yo'l bilan tarqatadilar: ular soxta xabarlarni "aytishda" yoki tvitlar yozishda davom etadilar va ular ijtimoiy tarmoqdagi haqiqiy foydalanuvchilarning postlariga javob berish yoki sharhlash uchun bir xil yolg'on ma'lumotlardan foydalanadilar.

Botlarning taktikasi ishlaydi, chunki oddiy ijtimoiy tarmoq foydalanuvchilari Facebookda, Twitterda retvitlar, trendli heshteglar, so'roqsiz (yoki bu holatda ma'lumot manbasining foydalanuvchi profiliga diqqat bilan qarab) o'zlari ko'rgan yoki boshqalar orasida baham ko'rilgan narsalarga ishonishadi. Shunday qilib, botlar bundan katta hajmdagi soxta yangiliklarni tarqatish va uni ishonchli ko'rsatish orqali foydalanadi [4], [5]. Ammo botlar boshqa foydalanuvchilar tomonidan qanday asl izohlarni retvit qilishni tanlashda unchalik yaxshi emas. Ular odamlardan unchalik aqlli emas. Ammo odamlar hissiyotga moyil. Soxta yangiliklar tarqalishida haqiqiy odamlarning o'zi ham katta rol o'ynaydi. Soxta yangiliklarni tarqatishda botlarning roli haqida ma'lumot paydo bo'lgach, ijtimoiy media kompaniyalari o'z platformalarida botlar va soxta akkauntlar mavjudligini kamaytirishga harakat qilishdi. Misol uchun, 2018-yil iyul oyida Twitter "o'n millionlab shubhali akkauntlarni o'chirishni" boshladi [6]. Botlar hali ham mavjud, lekin ko'pincha soxta yangiliklarning tarqalishi haqiqiy odamlarning yosh bolalarcha tutgan ishining natijasi. Bizning barchamiz, muammoning eng katta qismi bo'lish ehtimoli bor foydalanuvchilarmiz.

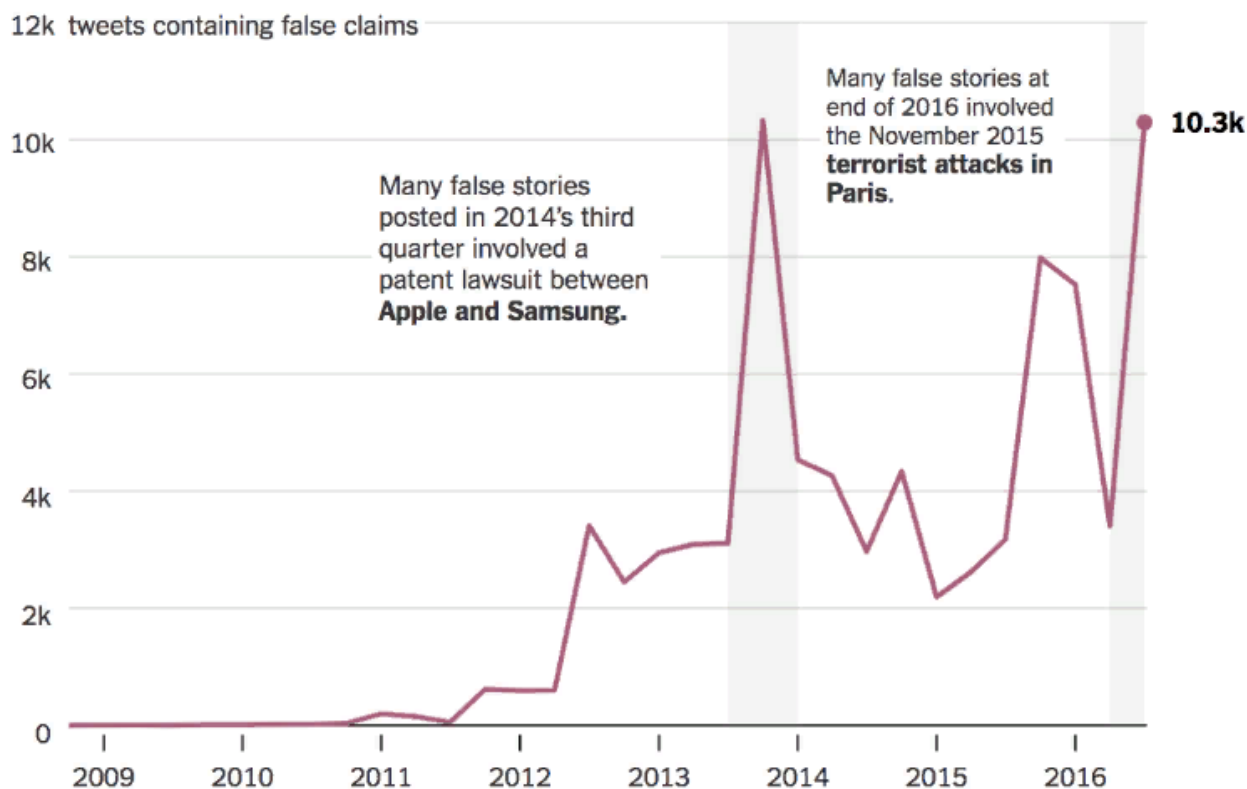
**Haqiqiy odamlar va feyk yangiliklar propagandasi.** Botlar ko'plab soxta xabarlarni tarqatayotgan bo'lsa-da, soxta xabarlarni qayta uzatishning aksariyati haqiqiy odamlar tomonidan sodir etiladi [7]. Odamlarni soxta yangiliklarga moyil qiladigan ijtimoiy mediadagi asosiy narsa – bu ijtimoiy tarmoq saytlari taqdim etadigan mashhurlik ko'rsatkichlari bo'lib, odamlar boshqa foydalanuvchilarga xabarni tasdiqlatish uchun bundan foydalanadilar. Tadqiqotlar shuni ko'rsatadiki, psixologik jihatdan Facebook postni ko'proq yoqtiradi, YouTube'dagi videoga ko'proq "bosh barmog'i" ovoz beradi yoki Yahoo!da ko'proq rozilik belgisi bo'ladi! Kimningdir sharhidagi foydali degan javoblar, boshqa o'quvchilarning xabar sifati haqidagi

tasavvurlarini o'zgartiradi va xabardagi asosiy masala haqidagi fikrlarini o'zgartiradilar [8], [9]. Tandoc va boshqalar tomonidan qilingan tadqiqot mashhurlik ko'rsatkichlari bo'yicha qo'shimcha ijtimoiy dinamikani taklif qiladi: "Agar post ko'p yoqtirishlar, ulashishlar yoki sharhlarga ega bo'lsa, u boshqalar tomonidan ko'proq e'tiborga olinadi va shuning uchun uni yoqtirish, baham ko'rish yoki sharhlash ehtimoli ko'proq" [10]. Yangiliklar yolg'onmi yoki yo'qmi, bu uning tagidagi sharhlar namunasida, ular haqiqatdir.

Ammo tadqiqotlar shuni ko'rsatadiki, odamlar turli sabablarga ko'ra haqiqiy yangiliklardan ko'ra soxta yangiliklarni baham ko'rishadi. Tadqiqotlar ko'ra, oddiy odamlar yolg'on xabarlarini aniqlashda qiynaladi va ular o'zlarining bunday qobiliyatsizligini tan olmaydilar [11]. Onlayn yangiliklar haqida gap ketganda, biz "haqiqiy"ni soxtadan ajrata olish qobiliyatiga haddan tashqari ishonamiz. Bu haddan tashqari ishonch ijtimoiy media platformalarida soxta yangiliklarni almashish imkoniyatini oshiradi. Vosoughi va boshqalar[7] haqiqiy Twitter foydalanuvchilarining soxta yangiliklarni retvit qilish ehtimoli haqiqatga yaqin yangiliklarga qaraganda 70% ko'proq ekanligini aniqladi. Odamlar yangilikni yaxshi ko'radilar va uni boshqalar bilan baham ko'rishni sevadilar. Soxta yangiliklar – ular tasvirlagan voqealar yoki bayonotlar hech qachon sodir bo'lmagani uchun har doim yangilikdir!

Keyinchalik, Vosoughi va boshqalarning tadqiqotlari ijtimoiy tarmoqlarda yangiliklarni baham ko'rishda hissiyotlarning rolini ta'kidladi. Ular haqiqiy yangiliklarni o'qish asosan quvonch, baxtsizlik, kutish va ishonch tuyg'ularini keltirib chiqarishini aniqladilar. Soxta yangiliklarni o'qish hayrat, xavotir, zarba va jirkanish tuyg'ularini keltirib chiqaradi. Tadqiqotchilar ushbu his-tuyg'ular ijtimoiy tarmoqlarda nimanidir baham ko'rishga qaror qilishda muhim rol o'ynashini aytishadi.

Ijtimoiy tarmoq foydalanuvchilari nafaqat siyosiy mavzularni baham ko'rishadi, texnologiya, shahar afsonalari, ilm-fan va biznesga oid soxta yangiliklar ham odamlar tomonidan keng tarqatilgan. Vosoughi va boshqalarning tadqiqotlariga asoslanib, New York Times 2010 va 2016-yillar oralig'ida Twitterda soxta yangiliklar mavzusining eng katta tendensiyalarini ko'rsatadigan jadvalni (quyida) tuzdi, bu siyosatdan boshqa mavzular ham ataylab noto'g'ri ma'lumotlarga duchor bo'lishini ko'rsatadi [12].



Rasm manbasi: New York Times

**Mikrotargeting va feyk yangiliklarni tarqatish.** Qanday qilib soxta yangiliklar ma'lum turdagi odamlarga yo'naltiriladi?

Qanday qilib soxta yangiliklar veb-saytlari o'z auditoriyasini nishonga oladi va ular yuborgan noto'g'ri ma'lumotlarni odamlar qabul qilishiga ishonch hosil qiladi? Buning usullaridan biri ijtimoiy media tahlilidan foydalanishdir [13]. Analitika qanday ishlashini tushunish uchun biz cookie-fayllar qanday ishlashini tushuntirishimiz, keyin esa ular o'z xabarlarini qabul qiluvchi auditoriyani topish uchun cookie-fayllar taqdim etgan ma'lumotlardan foydalanishga guruhlarini qanday qiziqtirishini ko'rsatishimiz kerak



Manba: OStraining.com

Cookie-fayllar haqida eshitgan bo'lsangiz kerak: afzal ko'rgan narsalaringizni, xaridlaringizni va hokazolarni eslab qolish uchun veb-saytlar kompyuteringizga o'rnatadigan fayllar. Siz tashrif buyurgan veb-saytga ilova yoki veb-brauzeringizga cookie-fayllarni o'rnatishiga rozilik berganingizdan keyin, siz ma'lum tanlovlarni amalga oshirganingizda (masalan, qaysi tilni afzal ko'rasiz) cookie veb-saytga yana tashrif buyurganingizda xuddi shu sozlamadan foydalanishni aytadi. Veb-saytlar bu siz ekanligingizni bilishadi, chunki brauzeringizda saqlangan cookie noyob identifikatorga ega. Shunga qaramay, veb-saytlar sizning qulayligingiz uchun faqat kompyuteringizda cookie-fayllarni saqlamaydi. Kompyuter tizimingizdagi cookie-fayllar siz tashrif buyurgan barcha veb-saytlar bo'ylab vebdagi harakatlaringizni ham kuzatib boradi. Siz saqlagan ba'zi cookie-fayllar siz tashrif buyurganlardan tashqari boshqa veb-saytlardan ham keladi. Kompyuteringizda "uchinchi tomon" deb ataladigan cookie-fayllarni saqlash uchun sozlangan har bir veb-sayt brauzeringiz cookie-fayllarining noyob identifikatori bilan aniqlangan - ularga tashrif buyurganligi haqida xabar beradi. Ushbu cookie-fayllar kuzatuv cookie-fayllari yoki qisqacha trekerlar deb ataladi. Siz so'rashingiz mumkin, kim sizning har bir qadamingizni Internetda kuzatishdan manfaatdor?

Ko'pgina kuzatuv cookie-fayllari reklamalarni shaxsiylashtirish uchun veb-sayt foydalanuvlarini to'playdigan va tahlil qiladigan kompaniyalardan keladi. Masalan, Facebookni olaylik. Facebookdan boshqa ko'plab veb-saytlarda Facebookning yoqtirish tugmasi mavjud. Har safar kimdir Facebook tugmasi paydo bo'lgan veb-saytga tashrif buyurganida, o'sha veb-sayt (aniqrog'i, tugma ekraningizdagi ko'rinishi bilan bog'liq bo'lgan dasturlash kodi) sizning Facebookka tashrifingiz haqida xabar beradi. Bu siz yoqtirish tugmachasini bosasizmi yoki bosmaysizmi, Facebookka kirganmisiz yoki yo'qmi, hatto Facebook foydalanuvchisi bo'lasizmi yo'qmi sodir bo'ladi. Veb-sayt egalari uchun afzallik shundaki, foydalanuvchilar o'z veb-sayti yoki postini yoqtirsa, ular kengroq auditoriyani qamrab olishi mumkin. Bundan tashqari, ular veb-saytlariga kim tashrif buyurganini bilish uchun Facebook hisobotlariga qarashlari mumkin [14].

Facebook, Google va boshqa kuzatuvchilar bilan ta'minlovchi veb-saytlar siz tashrif buyurgan veb-saytlarni, shuningdek, ushbu veb-saytlarni ko'rganingizda nima qilganingizni – nimani bosganingiz, u yerda qancha vaqt o'tkazganingiz, boshqa qanday sahifalarni ochganingiz va hokazolarni tahlil qiladi.— brauzeringizda siz hatto bilmagan skriptlarni (kichik dasturlarni) ishga tushirish orqali buni amalga oshiradi[15]. Siz tashrif buyurgan veb-saytlar ushbu veb-saytlarda qilgan harakatlaringiz bilan birgalikda boshqa ijtimoiy media tahlil firmalariga siz haqingizda

qimmatli ma'lumotlarni beradi. Ushbu ma'lumotlarga asoslanib, ular sizning qiziqishlaringiz va xarid qilish modellaringizni bashorat qilish, sizga ijobiy munosabatda bo'lish ehtimoli yuqori bo'lgan reklama turlarini tanlash va yetkazib berish uchun modellarni hisoblab chiqadi. Facebook esa siz boshqa veb-saytlarda ko'rgan mahsulotlarni reklama qilish uchun kompaniyalarga reklama sotishi mumkin. Hech qachon poyabzal sotadigan veb-saytda poyabzalga qaraganmisiz, keyin esa keyingi safar Google yoki Facebookdan foydalanganingizda poyabzal reklamalarini ko'rganmisiz? Cookie shunday parchalanadi.

Ba'zi odamlar o'zlarining ma'lumotlari o'zlari yoqtirgan mahsulotlar reklamalarini ko'rsatish va bu reklamalar ularga yanada jozibali ko'rinish uchun ishlatilishiga qarshi bo'lmasa-da, boshqalari bu amaliyotga qarshi. Bu yerda uchta tashvishni eslatib o'tishimiz kerak. Birinchisi, ma'lumotlarni yig'ishning o'zi haqida. Aksariyat odamlar ular haqida qanday ma'lumotlar to'planganiga to'liq ishonch hosil qilishmaydi va bu qoida tariqasida, ularga yoqmaydi. Ikkinchi, tashvish maxfiylik bilan bog'liq. Maxfiylik himoyachilarining ko'pchiligi iste'molchilarga ma'lumotlar kim bilan bo'lishishi va kompaniya ularni to'plaganidan keyin odamlar o'z ma'lumotlarini qanchalik nazorat qilishlari noma'lum ekanligini ta'kidlaydilar. Xakerlar shaxsiy ma'lumotlarni o'g'irlashadi va ba'zan hatto e'lon qilishadi, bu ma'lumotlar to'planganidan keyin uning xavfsizligi haqida tashvish tug'diradi [16].

Uchinchi tashvish ma'lumotlar nima qilish uchun ishlatilishi bilan bog'liq. Ba'zi media-tahlil firmalari sizga poyabzal, yangi noutbuk yoki telefon kabi mahsulotni sotmoqchi emas. Sizni siyosiy nomzodga ovoz berishga ishontirish uchun ma'lumotlaringizni tahlil qilishga ixtisoslashgan ba'zi firmalar mavjud. Bu ba'zi jihatdan eski moda reklama kompaniyasi strategiyalariga o'xshash bo'lsa-da, ijtimoiy media tahlillari kompaniyalarga sizni aniqroq yo'naltirishga imkon beradi. Ular qanday qilib "tugmachalaringizni bosishni" biladilar va muammolar va nomzodlarning ushbu masalalar bo'yicha pozitsiyasidan kelib chiqib, sizni u yoki bu nomzodga ovoz berishga ishontirishga harakat qilishadi, ularda sizga va siz kabi boshqalarga murojaat qilishga, ishontirishga asos bor. Ular internet yoki ijtimoiy mediadan foydalanganingizda sizni reklamalar yoki soxta yangiliklar ko'rishga majbur qilishlari mumkin.

## XULOSA

Agar siz ushbu hikoyalar yoki reklamalarga javob bersangiz, masalan, ularni yoqtirsangiz yoki ularga sharh bersangiz, sizning afzalliklaringiz haqidagi ma'lumotlar yanada aniq va aniqroq bo'ladi. Shuni ta'kidlash kerakki, media platformalar aslida sizga nimani ko'rsatishni hal qilmaydi. Lekin ular sizning afzalliklaringiz va assotsiatsiyalaringiz profilingizni bilishadi va ular reklama beruvchilarga sizning

afzalliklaringiz va birlashmalarining baham ko'radigan sizga o'xshagan odamlarga kirish huquqini sotadilar va reklama beruvchilarning xabarlarini ijtimoiy media platformasi orqali avtomatik ravishda sizga ko'rsatiladi. [17]. Facebookning reklama algoritmlari bu pullik reklamalar kimga ko'rsatilishini aniqlaydi, ularning ba'zilari soxta yangiliklar bo'lishi mumkin, odamlarning siyosiy yoki boshqa e'tiqodlariga ta'sir qilish uchun mo'ljallangan. "Mikrotargeting" - bu muayyan xabarlarni o'qishi, yoqtirishi va baham ko'rishi va u paydo bo'lgan (soxta yangiliklar yoki boshqa) veb-saytlarga kirishi mumkin bo'lgan odamlarga ma'lum xabarlarni ko'rsatish uchun ma'lumotlardan foydalanish atamasi.

**Trollar va soxta yangiliklarning tarqalishi.** Trollar, ijtimoiy media platformalarida ko'proq yoki kamroq miqdorda bir maqsadda yaratilgan akkauntlarga ega bo'lgan odamlardir: odamlar bilan bahslashadigan, boshqa foydalanuvchilar va jamoat arboblarni haqorat qiladigan va ularga ism qo'yadigan sharhlar yaratish, ular g'oyalari ishonchni susaytirishga harakat qilish, yoqtirmaslik va bu g'oyalarni joylashtirgan shaxslarni qo'rqitish kabi ishlarni amalga oshiradilar. Va ular mafkuraviy jihatdan mos keladigan soxta yangiliklarni qo'llab-quvvatlaydilar va himoya qiladilar. Ular ko'pincha sharhlarida juda qo'pol bo'ladi. Va bu boshqa normal foydalanuvchilarni ham qo'polikka undaydi. 2016-yilgi AQSh saylovlariga ta'sir ko'rsatish uchun ko'plab yolg'on xabarlar tarqatgan Rossiya Internet tadqiqotlari agentligi yillar davomida trollarni qo'llab-quvvatlab keladi. Ularning o'z agentlari saylov kompaniyasi boshlanishidan ancha oldin ijtimoiy tarmoqlardagi akkauntlarini yaratgan, ular o'zlarining ijtimoiy tarmoqlardagi profillarini odatdagi amerikaliklarga o'xshatib qo'yganlar: ular amerikalik ismlarni tanlaganlar, o'zlarining (va ularning soxta oilalarining) fotosuratlarini va tavsiflarini internetga joylashtirganlar va ular nomi ostida ba'zi narsalarni yoqlashgan va muhokama guruhlariga qo'shilishgan. Ular bir muddat zararsiz xabarlar berishdi va do'stlar va izdoshlar orttirishdi. Ular Amerikaning ijtimoiy media maydoniga ozmi-ko'pmi kirib borishdi va saylov mavsumigacha pastda yotishdi. Keyin ular jirkanchlikni tarqatdilar, soxta yangiliklarni qo'llab-quvvatladilar va haqiqiy yangiliklarga ishonmaslikni kuchaytirdilar. Bularning barchasi Kongress tergovlarida va Robert Myullerning Rossiya tomonidan 2016-yilgi saylovlarda mumkin bo'lgan qonunbuzarliklar bo'yicha tergov natijasida e'lon qilingan ayblovlarda juda yaxshi hujjatlashtirilgan [18]. Tashqi siyosat tadqiqot instituti xodimi Klint Uottsning AQSh Senati quyi qo'mitasiga taqdimotidan boshlab Rossiyaning Ijtimoiy tarmoqlarga ta'sir ko'rsatish operatsiyalari haqida qisqacha ma'lumot:

Hamma trollar rus o'simliklari emas. O'zimizda yetishtirilgan navimiz ham bor [19]. Biz ular haqida kamroq ma'lumotga egamiz, chunki ular qilayotgan ishlari



noqonuniy emas va ular rasmiy ravishda tekshirilmagan. Hali ham mavjud bo'lgan rus trollari va ularning ta'siridan qochish uchun nima qilish kerakligi haqida ko'proq bilish uchun ACT.TV-dan ushbu 3 daqiqalik videoni tavsiya qilamiz: <https://youtu.be/psmpWVuCb8s>

### FOYDALANILGAN ADABIYOTLAR RO'YXATI:

1. C. A. de L. S. Berente Nikolas, "Bu ijtimoiy bot axloqsiz ish tutyaptimi?", ACM xabarlar, jild. 60, yo'q. 9, 29–31-betlar, 2017 yil sentyabr, <https://10.1145/3126492>.
2. Y. Boshmaf, I. Musluxov, K. Beznosov va M. Ripeanu, "Ijtimoiy botnetni loyihalash va tahlil qilish", Kompyuter tarmoqlari: Kompyuter va telekommunikatsiya tarmoqlari xalqaro jurnali, jild. 57, yo'q. 2, 556–578-bet, 2013 yil fevral, <https://10.1016/j.comnet.2012.06.006>.
3. F. Morstatter, L. Vu, T. H. Nazer, K. M. Karli va X. Liu, "Botni aniqlashga yangi yondashuv: aniqlik va eslab qolish o'rtasidagi muvozanatni saqlash", 2016 yilda IEEE/ACM ijtimoiy sohadagi yutuqlar bo'yicha xalqaro konferentsiya Tarmoqlarni tahlil qilish va qazib olish (ASONAM), 2016 yil avgust, 533–540-betlar. <https://10.1109/ASONAM.2016.7752287>.
4. E. Ferrara, O. Varol, C. Davis, F. Menczer va A. Flammini, "The Rise of Social Bots", Communications of ACM, vol. 59, yo'q. 7, 96–104-betlar, 2016 yil iyun, <https://10.1145/2818717>.
5. C. Vatt, ekstremistik tarkib va rus tilidagi dezinformatsiyalar: Yechimlarni topish uchun texnologiya bilan ishlash. 2017. Kirilgan: 2018 yil 02 avgust. [Onlayn]. Mavjud:<https://www.judiciary.senate.gov/imo/media/doc/10-3117%20Watts%20Testimony.pdf>
6. N. Confessore va G. J. X. Dance, "Soxta akkauntlarga qarshi kurash, Twitter millionlab obunachilarni kesish uchun", The New York Times, 13-iyul, 2018-yil. <https://www.nytimes.com/2018/07/11/Technology/twitter-fake-followers.html> (2018-yil 02-avgust).
7. S. Vosoughi, D. Roy va S. Aral, "The Spread of True and False News Internet", Science, jild. 359, yo'q. 6380, 1146–1151-betlar, 2018 yil mart, <https://10.1126/science.aap9559>.
8. J. B. Valter va J. Jang, "Ishtirokchi veb-saytlardagi aloqa jarayonlari", Journal of Computer-mediated Communication, jild. 18, yo'q. 1, 2–15-betlar, 2012 yil oktyabr, <https://10.1111/j.1083-6101.2012.01592.x>.
9. J. B. Valter, J. Jang va A. A. H. Edwards, "Veb 2.0 muhitida salomatlik bo'yicha maslahatlarni baholash: foydalanuvchilar tomonidan yaratilgan bir nechta omillarning

- OIV bo'yicha maslahatlarni qabul qilishga ta'siri," Health Communication, jild. 33, yo'q. 1, 57–67-betlar, 2018 yil yanvar, <https://10.1080/10410236.2016.1242036>.
10. E. C. Tandok, Z. V. Lim va R. Ling, "Fake News"ni aniqlash: ilmiy ta'riflar tipologiyasi, raqamli jurnalistika, jild. 6, yo'q. 2, 137–153-betlar, 2018 yil fevral, <https://10.1080/21670811.2017.1360143>.
11. B. A. Lyons, J. M. Montgomeri, A. M. Guess, B. Nyhan va J. Reifler, "Yangiliklar hukmlariga haddan tashqari ishonch yolg'on xabarlar sezgirlik bilan bog'liq", Milliy Fanlar Akademiyasi materiallari, jild. 118, yo'q. 23, p. e2019527118, 2021 yil iyun, <https://10.1073/pnas.2019527118>.
12. S. Lohr, "To'g'ri: yolg'on xabarlar tezroq va kengroq tarqaladi. Va odamlar aybdor", The New York Times, 08-iyun, 2018-yil. <https://www.nytimes.com/2018/03/08/technology/twitter-fake-news-research.html> (kirish 02-avgust. , 2018).
13. "Ijtimoiy Media Analytics (SMA) nima?" texnopediya. <https://www.techopedia.com/definition/13853/social-media-analytics-sma> (kirish 2018-yil 2-avgust).
14. D. Nield, "Siz, ehtimol, Facebook sizni kuzatadigan barcha usullarni bilmassiz", Gizmodo, 08-iyun, 2017-yil. <https://fieldguide.gizmodo.com/all-the-ways-facebook-tracks-you-that-that-you-might-no-1795604150> (kirish 2018-yil 02-avgust).
15. N. Tiku, "Siz veb-saytni ko'rib chiqyapsiz. Bu kompaniyalar sizning har bir harakatingizni yozib olishlari mumkin," Wired, 2017-yil 16-noyabr. <https://www.wired.com/story/the-dark-side-of-replay-sessions-that-record-your-every-move-online/> (2018-yil 02-avgust).
16. M. Curtin, "Facebook ma'lumotlaringiz Cambridge Analytica tomonidan o'g'irlanganmi? Mana buni qanday aytish mumkin," Inc.com, 11-aprel, 2018-yil. <https://www.inc.com/melanie-curtin/was-your-facebook-data-stolen-by-cambridge-analytica-heres-how-to-tell.html> (2018-yil 02-avgust).
17. J. Olbrayt, "#Election2016: Propaganda-lytics & Weaponized Shadow Trackers," Medium, 22-noyabr, 2016-yil. <https://medium.com/@d1gi/election2016-propaganda-lytics-weaponized-shadow-trackers-a6c9281f5ef9> (2018-yil 02-avgust).
18. Amerika Qo'shma Shtatlari v. Internet Research Agency va boshqalar. 2018. [Onlayn]. Mavjud: <https://www.justice.gov/file/1035477/download>
19. L. Bénichou, "Internetning eng zaharli trollari ... Vermontda yashaydimi?", Wired, 22-avgust, 2017-yil. Kirish: 07-avgust, 2018-yil. [Onlayn]. Mavjud: <https://www.wired.com/2017/08/internet-troll-map/>