QO‘QON DAVLAT PEDAGOGIKA INSTITUTI ILMIY XABARLARI
(2025-yil 2-son)

FILOLOGIYA

PHILOLOGY

ZAMONAVIY INTERNET JURNALISTIKASI VA MA’LUMOTLAR XAVFSIZLIGI: AXBOROT XAVFSIZLIGI VA JURNALISTLARNING HIMOYASI

Sadullayeva Oybarchin Mirolim qizi
Samarqand davlat chet tillar instituti
Jurnalistika yo‘nalishi 2-bosqich talabasi.
oybarchinsadullayeva@gmail.com
910304003
G‘aybullayev Otabek Muhammadiyevich
Ilmiy ishlar va innovatsiyalar bo‘yicha prorektor,
falsafa fanlari doktori , professor

Abstract Ushbu maqola internet jurnalistikasi va axborot xavfsizligi o‘rtasidagi bog‘liqlikni tahlil qiladi hamda jurnalistlarning axborot xavfsizligini ta’minlash bo‘yicha samarali strategiyalarni o‘rganadi. Xavfsiz kommunikatsiya vositalari, parol menejmenti, ishonchli axborot manbalarini tekshirish va maxfiy ma’lumotlarni himoyalash kabi choralar muhokama qilinadi. Tadqiqot natijalari shuni ko‘rsatadiki, jurnalistlarning kiberxavfsizlikni mustahkamlash choralari mustaqil va ishonchli jurnalistikaning rivojlanishiga xizmat qiladi.

Kalit so‘zlar: internet jurnalistikasi, kiberxavfsizlik, dezinformatsiya, jurnalistlarning himoyasi, axborot xavfsizligi.

СОВРЕМЕННАЯ ИНТЕРНЕТ-ЖУРНАЛИСТИКА И БЕЗОПАСНОСТЬ ДАННЫХ: ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ЖУРНАЛИСТОВ

Аннотация В данной статье анализируется взаимосвязь между интернет-журналистикой и информационной безопасностью, а также рассматриваются эффективные стратегии обеспечения информационной безопасности журналистов. Обсуждаются такие меры, как использование защищённых средств коммуникации, управление паролями, проверка достоверных источников информации и защита конфиденциальных данных. Результаты исследования показывают, что усиление мер кибербезопасности журналистов способствует развитию независимой и надёжной журналистики.

Ключевые слова: интернет-журналистика, кибербезопасность, дезинформация, защита журналистов, информационная безопасность.

MODERN INTERNET JOURNALISM AND DATA SECURITY: INFORMATION SECURITY AND JOURNALISTS’ PROTECTION

Abstract This article analyzes the relationship between online journalism and information security and explores effective strategies for ensuring journalists' information security. Measures such as secure communication tools, password management, verification of reliable information sources, and protection of confidential data are discussed. The research results indicate that strengthening journalists' cybersecurity measures contributes to the development of independent and reliable journalism.

Keywords: online journalism, cybersecurity, disinformation, journalists' protection, information security.

Kirish

Internet jurnalistikasi so‘nggi o‘n yilliklarda global axborot maydonining muhim qismi sifatida shakllandi. Raqamli texnologiyalar rivojlanishi natijasida yangiliklar tarqatish tezlashdi, auditoriya ko‘lami kengaydi va ommaviy axborot vositalarining ta’siri kuchaydi. Jurnalistlar internet orqali keng ko‘lamli axborotni tarqatish, faktlarni tezkor tekshirish va auditoriya bilan bevosita aloqa o‘rnatish imkoniyatiga ega bo‘ldilar. Biroq, ushbu taraqqiyot kiberxavfsizlik bilan bog‘liq yangi muammolarni ham keltirib chiqardi. Internet jurnalistlari hozirgi kunda turli tahdidlarga duch kelmoqda. Kiberjinoyatchilar tomonidan amalga oshiriladigan fishing hujumlari, hisoblarni buzish, shaxsiy ma’lumotlarni oshkor qilish (doxxing), shaxsiy yoki kasbiy faoliyatga to‘sqinlik qilish maqsadida qaratilgan hujumlar tobora keng tarqalmoqda. Shuningdek, dezinformatsiya va axborot manipulyatsiyasi internet jurnalistikasining ishonchliligiga putur yetkazmoqda. Mazkur maqola internet jurnalistikasi bilan bog‘liq axborot xavfsizligi muammolarini o‘rganishga qaratilgan. Jurnalistlarga qaratilgan asosiy tahdidlar va ularning oldini olish usullari tahlil qilinadi. Shuningdek, jurnalistlarning axborot xavfsizligini ta’minlash uchun qo‘llashi mumkin bo‘lgan strategiyalar, jumladan, xavfsiz kommunikatsiya vositalaridan foydalanish, parol menejmenti, ishonchli manbalarni tekshirish va maxfiy ma’lumotlarni himoyalash kabi choralar ko‘rib chiqiladi.

Raqamli texnologiyalarni joriy etish – zamon talabi. Biz iqtisodiyot va ijtimoiy sohalarni tubdan isloh qilish uchun ‘Raqamli O‘zbekiston – 2030’ dasturini amalga oshiryapmiz [1].

Internet jurnalistikasi va axborot xavfsizligiga tahdidlar

Fishing hujumlari jurnalistlarga qarshi ishlatiladigan eng keng tarqalgan tajovuzkor usullardan biri bo‘lib, bu orqali tajovuzkorlar shaxsiy ma’lumotlarni qo‘lga kiritishga harakat qiladi. Ushbu hujumlar odatda soxta elektron pochta xabarlari, xakerlik yo‘li bilan olingan login va parollar, yoki ijtimoiy tarmoqlardagi manipulyatsiyalar orqali amalga oshiriladi. Ijtimoiy muhandislik esa odamlarning ongini boshqarish orqali maxfiy ma’lumotlarni olish usulidir. Jurnalistlarga nisbatan bunday hujumlar ularning ishonchiga kirib, ma’lumotlarni ochib berishga undash orqali amalga oshiriladi. Bunday tahdidlardan himoyalanish uchun jurnalistlar har qanday shubhali havolalar va elektron xatlarni ehtiyotkorlik bilan tekshirishlari kerak.

DDoS (Distributed Denial of Service) hujumlari mustaqil jurnalistlar va ommaviy axborot vositalari saytlariga qarshi tez-tez ishlatiladigan vositalardan biri hisoblanadi [2]. Ushbu hujumlar serverlarga ortiqcha yuklama yuklash orqali veb-saytlarning faoliyatini izdan chiqaradi. Ko‘plab hukumatlar va siyosiy manfaatdor tomonlar DDoS hujumlaridan norasmiy tsenzura vositasi sifatida foydalanishadi. Jurnalistlar va media tashkilotlari bunday tahdidlardan himoyalanish uchun Cloudflare kabi xavfsizlik xizmatlaridan foydalanishlari, shuningdek, maqolalarning zaxira nusxalarini turli serverlarda saqlashlari kerak. Soxta yangiliklar va dezinformatsiya jurnalistlarning ishiga jiddiy zarar yetkazadigan tahdidlardan biridir. Dezinformatsiya botlar, yolg‘on ijtimoiy tarmoq akkauntlari va hatto sun’iy intellekt yordamida yaratilgan deepfake texnologiyalari orqali tarqatiladi. Bunday hujumlarning oldini olish uchun jurnalistlar Google Reverse Image Search, TinEye va fact-checking platformalaridan foydalanishlari, axborotni bir necha mustaqil manbadan tekshirishlari lozim [3].

Internet jurnalistikasi rivojlanishi bilan birga jurnalistlarning axborot xavfsizligiga bo‘lgan ehtiyoj ham oshib bormoqda. Kiberxavfsizlik tahdidlari jurnalistlar uchun nafaqat kasbiy, balki shaxsiy xavf tug‘diradi. Ayniqsa, mustaqil va tergov jurnalistlari uchun bu tahdidlar yanada jiddiy hisoblanadi. Kiberjinoyatchilar va hukumat nazorati ostidagi manipulyatsiya guruhlari jurnalistlarning hisoblarini buzish, ma’lumotlarini o‘g‘irlash yoki shaxsiy hayotiga doir ma’lumotlarni tarqatish orqali ularga bosim o‘tkazishga urinmoqda. Shu sababli jurnalistlar axborot xavfsizligini ta’minlash uchun zamonaviy texnologiyalardan samarali foydalanishlari lozim. Jurnalistlar duch keladigan asosiy xavflardan biri fishing hujumlari bo‘lib, bu firibgarlar tomonidan shaxsiy ma’lumotlarni qo‘lga kiritish maqsadida amalga oshiriladigan tajovuzkor texnikadir. Fishing hujumlari odatda elektron pochta, soxta veb-saytlar yoki ijtimoiy tarmoqlar orqali amalga oshiriladi. Shu sababli jurnalistlar har qanday shubhali havolalarni bosishdan oldin ularning haqiqiyligini tekshirishlari zarur. Bunday hujumlarning oldini olish uchun ikki faktorli autentifikatsiya (2FA) va shifrlangan elektron pochta xizmatlaridan foydalanish tavsiya etiladi.Bundan tashqari, jurnalistlarning ma’lumotlar bazalari va veb-saytlari DDoS hujumlariga ham uchrashi mumkin. Bu hujumlar serverlarga ortiqcha yuklama yuklash orqali veb-saytlarning ishdan chiqishiga sabab bo‘ladi. Mustaqil media tashkilotlari va jurnalistlar bunday tahdidlardan himoyalanish uchun Cloudflare kabi DDoS hujumlariga qarshi xizmatlardan foydalanishlari lozim. Shuningdek, jurnalistlar o‘z maqolalarining zaxira nusxalarini saqlash va xavfsiz serverlardan foydalanishlari kerak. Axborot xavfsizligiga yana bir katta tahdid – dezinformatsiya va yolg‘on yangiliklarning keng tarqalishi bilan bog‘liq. Bugungi kunda soxta yangiliklar turli internet platformalarida ommalashib, jamoatchilik fikriga salbiy ta’sir ko‘rsatmoqda. Feyk axborot tarqatishning keng tarqalgan usullari – ijtimoiy tarmoqlardagi botlar, deepfake texnologiyalari va noto‘g‘ri kontekstda taqdim etilgan ma’lumotlardir. Jurnalistlar ishonchli axborotni ommaga yetkazish uchun ma’lumotlarni bir necha manbadan tekshirishlari, fact-checking platformalaridan foydalanishlari va tasvirlarni tahlil qilish uchun Google Reverse Image Search yoki TinEye kabi vositalardan foydalanishlari lozim. Jurnalistlar o‘z xavfsizligini ta’minlash uchun maxfiy

hujjatlar bilan ishlashda ehtiyotkor bo‘lishlari shart. Ma’lumotlarning buzilishining oldini olish uchun shifrlangan saqlash texnologiyalaridan foydalanish zarur. Shifrlangan USB yoki xavfsiz serverlardan foydalanish jurnalistlarning maxfiy ma’lumotlarini himoya qilishga yordam beradi. Bundan tashqari, jurnalistlar o‘z manbalarining anonimligini saqlab qolish uchun shifrlangan aloqa vositalaridan, masalan, Signal yoki ProtonMail kabi xizmatlardan foydalanishlari kerak [4]. Internet jurnalistikasi bugungi jamiyatda axborot tarqatishning eng muhim vositalaridan biri hisoblanadi. Biroq, jurnalistlarning kiberxavfsizligini ta’minlash ularning faoliyatining samaradorligi va ishonchliligini oshirishda muhim ahamiyat kasb etadi. Jurnalistlarning axborot xavfsizligini mustahkamlash choralari mustaqil jurnalistikaning rivojlanishiga xizmat qiladi. Kiberjinoyatchilik va axborot manipulyatsiyasi tahdidlarining oldini olish uchun jurnalistlar zamonaviy texnologiyalardan samarali foydalanishlari, maxfiy ma’lumotlarni himoya qilish qoidalariga rioya qilishlari va xavfsizlik choralarini kuchaytirishlari shart. Bu esa nafaqat jurnalistlarning himoyasini ta’minlaydi, balki butun jamiyatning axborotga bo‘lgan ishonchini mustahkamlashga xizmat qiladi [5].

Jurnalistlar uchun kiberxavfsizlik choralarini mustahkamlash

Jurnalistlar shaxsiy va kasbiy ma’lumotlarini himoya qilish uchun shifrlangan aloqa vositalaridan foydalanishlari shart. Bunday vositalarga quyidagilar kiradi:

- **Signal** – shifrlangan xabar almashish ilovasi
- **ProtonMail** – shifrlangan elektron pochta xizmati
- **Tor Browser** – anonimlikni ta’minlaydigan brauzer
- **VPN xizmatlari** – internetga xavfsiz kirish uchun

Jurnalistlar o‘z hisoblarini himoya qilish uchun murakkab parollardan foydalanishlari va ularni xavfsiz saqlash uchun LastPass yoki Bitwarden kabi parol menejerlaridan foydalanishlari kerak. Bundan tashqari, ikki faktorli autentifikatsiya (2FA) akkauntlarni buzishning oldini oladi. Jurnalistlar o‘z manbalarining maxfiyligini saqlash uchun hujjatlarni shifrlashlari, bulutli xotira xizmatlari o‘rniga shaxsiy shifrlangan disklar yoki xavfsiz serverlardan foydalanishlari lozim. Shu bilan birga, anonim ma’lumot almashish uchun SecureDrop kabi tizimlar qo‘llanilishi tavsiya etiladi [6].

Jurnalistlar uchun maxfiy hujjatlarni himoya qilish juda muhim, chunki ular ko‘pincha maxfiy manbalar bilan ishlaydi va sezgir ma’lumotlarga ega bo‘ladi. Kiberjinoyatchilar, davlat organlari yoki boshqa manfaatdor guruhlar jurnalistlarning shaxsiy va ish bilan bog‘liq ma’lumotlarini qo‘lga kiritish uchun turli usullardan foydalanadilar. Shu sababli, jurnalistlar o‘zlarining ma’lumotlarini xavfsiz saqlash, shifrlash va himoyalash choralarini ko‘rishlari kerak. Buning uchun birinchi navbatda shifrlangan saqlash vositalaridan foydalanish zarur. Shifrlash ma’lumotlarni o‘g‘irlanish va buzilishlardan himoya qiladi. Masalan, **VeraCrypt** jurnalistlarga maxfiy fayllarini maxsus shifrlangan diskda saqlash imkonini beradi, **BitLocker** Windows foydalanuvchilari uchun disklarni shifrlash imkoniyatini taqdim etadi, **FileVault** esa Mac OS tizimlarida himoya vositasi bo‘lib xizmat qiladi. Bu vositalar jurnalistlarga kompyuter yoki tashqi xotira qurilmalaridagi ma’lumotlarini xavfsiz saqlashga yordam beradi. Bundan

tashqari, jurnalistlar o‘z hujjatlarini saqlash uchun bulutli xizmatlardan foydalanishda ehtiyot bo‘lishlari lozim. Google Drive yoki Dropbox kabi xizmatlar ba’zan yetarli darajada xavfsiz bo‘lmasligi mumkin. Shu sababli, shifrlangan va maxfiy saqlashni ta’minlaydigan bulut xizmatlaridan foydalanish tavsiya etiladi. **ProtonDrive**, **Tresorit** va **MEGA** kabi xizmatlar jurnalistlarga ma’lumotlarini shifrlangan holda saqlash imkoniyatini beradi. Bunday xizmatlardan foydalanganda, ikki faktorli autentifikatsiya (2FA) yoqilishi va kuchli parollar tanlanishi kerak. Jurnalistlarning ba’zi ma’lumotlarni maxfiy tarzda uzatish yoki ishonchli manbalardan qabul qilish zarurati ham bo‘lishi mumkin. Bunday hollarda, **SecureDrop** tizimi eng ishonchli usul hisoblanadi. Ushbu platforma maxfiy ma’lumotlarni jurnalistlarga anonim tarzda yetkazish imkonini beradi va hozirda ko‘plab nufuzli nashrlar, jumladan, **The Guardian** va **The Washington Post** undan foydalanadi [7]. Shuningdek, **OnionShare** xizmati Tor tarmog‘idan foydalangan holda shifrlangan ma’lumotlar almashish imkonini beradi, **PrivNote** esa vaqtinchalik maxfiy xabarlarni yuborish uchun ishlatilishi mumkin. Bundan tashqari, jurnalistlar o‘z ma’lumotlarini zaxiralashga ham e’tibor qaratishlari kerak. Muhim hujjatlar, fotosuratlar yoki videolar yo‘qolib qolmasligi uchun ularni tashqi qattiq diskda, shifrlangan USB fleshkalarida yoki maxsus serverlarda saqlash lozim. Ma’lumotlar buzilganda yoki o‘chirilganda ularni tiklash imkoniyati bo‘lishi uchun jurnalistlar o‘z ma’lumotlarini muntazam ravishda zaxiralashlari kerak [8]. Shu bilan birga, bunday zaxira nusxalari o‘g‘irlanish yoki buzilish xavfidan himoyalangan bo‘lishi shart. **Cryptomator** kabi shifrlash vositalari zaxiralangan ma’lumotlarni qo‘shimcha himoya bilan ta’minlashi mumkin. Jurnalistlar o‘zlarining maxfiy hujjatlari va ma’lumotlarini himoya qilish uchun yuqorida keltirilgan vositalardan foydalanishlari, xavfsizlik choralari haqida muntazam ma’lumotga ega bo‘lishlari va ehtiyotkorlik bilan ishlashlari zarur. Shaxsiy ma’lumotlarning buzilishi yoki tarqalib ketishi jurnalistning ishi va hayotiga jiddiy xavf tug‘dirishi mumkin. Shu sababli, maxfiy hujjatlarni himoya qilish har bir jurnalist uchun muhim vazifa bo‘lishi kerak [9].

Xulosa

Zamonaviy internet jurnalistikasi axborot tarqatishning eng tezkor va samarali vositasiga aylangan bo‘lsa-da, u bilan bog‘liq axborot xavfsizligi muammolari ham ortib bormoqda. Jurnalistlar kiberjinoyatchilik, dezinformatsiya, shaxsiy ma’lumotlarning oshkor bo‘lishi va raqamli kuzatuv tahdidlariga duch kelmoqda. Ayniqsa, mustaqil va tergov jurnalistlari uchun bu tahdidlar yanada keskin bo‘lib, ularning kasbiy faoliyatiga jiddiy ta’sir ko‘rsatishi mumkin. Ushbu maqolada internet jurnalistikasi bilan bog‘liq asosiy axborot xavfsizligi muammolari va ularning oldini olish choralari tahlil qilindi. Jurnalistlar o‘z ma’lumotlarini himoya qilish uchun xavfsiz kommunikatsiya vositalaridan foydalanishlari, ikki faktorli autentifikatsiya va parol menejerlarini qo‘llashlari, shuningdek, dezinformatsiyaga qarshi kurashish uchun fact-checking texnologiyalaridan foydalanishlari lozimligi ta’kidlandi. Axborot xavfsizligini ta’minlash faqat jurnalistlarning shaxsiy xavfsizligi bilan cheklanmaydi, balki butun jamiyatning ishonchli axborotga ega bo‘lish huquqini himoya qilishga xizmat qiladi. Internet jurnalistikasi axborot erkinligini mustahkamlashda katta rol o‘ynaydi, ammo jurnalistlarning kiberxavfsizlik

choralariga e’tibor bermasligi ularning ishonchliligi va faoliyatiga jiddiy xavf tug‘dirishi mumkin. Kelajakda jurnalistlar va ommaviy axborot vositalari axborot xavfsizligini oshirish bo‘yicha yangi texnologiyalarni joriy etishlari va xavfsizlik madaniyatini rivojlantirishlari lozim. Shuningdek, hukumat va nodavlat tashkilotlar jurnalistlarning himoyasini ta’minlash uchun qo‘shimcha qonuniy va texnik choralar ishlab chiqishlari zarur.Umuman olganda, internet jurnalistikasi va axborot xavfsizligi o‘zaro bog‘liq bo‘lib, jurnalistlarning himoyasini mustahkamlash nafaqat ularning kasbiy faoliyatini qo‘llab-quvvatlash, balki jamiyatning sifatli axborot olish huquqini ta’minlash uchun ham muhim ahamiyat kasb etadi. Shu sababli jurnalistlar kib erxavfsizlik choralarini mustahkamlashlari, axborot manbalarining ishonchliligini tekshirishlari va o‘zlarining shaxsiy ma’lumotlarini himoya qilish uchun ilg‘or texnologiyalardan foydalanishlari lozim.

FOYDALANILGAN ADABIYOTLAR

1. Mirziyoyev, Shavkat. *Raqamli iqtisodiyot va innovatsiyalar bo‘yicha yig‘ilishdagi nutq*. 5 okt. 2020.
2. Abdurahmonov, K. "OAVda axborot xavfsizligini ta’minlashning dolzarb masalalari." *Axborot texnologiyalari va tizimlari*, 2021,
3. Electronic Frontier Foundation. *Surveillance Self-Defense: A Guide to Protecting Yourself from Online Tracking*. https://ssd.eff.org/ 2022.
4. Greenberg, A. *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin’s Most Dangerous Hackers*. Doubleday. 2019.
5. Ismoilova, D. "Internet jurnalistikasi va dezinformatsiya: feyk yangiliklarga qarshi kurash usullari." *O‘zbekiston Jurnalistika Ilmiy Jurnali*, 2022,
6. Karimov, O. "Raqamli media muhitida jurnalistlarning kiberxavfsizligi: tahdidlar va himoya strategiyalari." *Axborot jamiyati tadqiqotlari*, 2023.
7. Schneier, B. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W. W. Norton & Company. 2015.
8. Zuboff, S. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs. 2019.