INTERNET JURNALISTIKA XAVFSIZLIGI: RAQAMLI TAHDIDLAR SHAROITIDA AXBOROT ISHLAB CHIQARISH, UZATISH VA HIMOYALASH MEXANIZMLARINING KOMPLEKS TAHLILI

Sharafatdinova Malika Berdaq qizi
Berdaq nomidagi Qoaqalpoq davlat universiteti
Qoraqalpoq filologiyasi va Jurnalistika fakuleteti
malikasharafatdinova8@gmail.com
+998 99 330 63 45
Doi: https://doi.org/10.5281/zenodo.20321019

Annotatsiya. Ushbu tezis internet jurnalistikasida xavfsizlik muammolarini tahririyat jarayonlari, texnologik infratuzilma va auditoriya bilan muloqot kontekstida ilmiy tahlil qiladi. Tadqiqot maqsadi raqamli tahdidlar tasnifi, ularning axborot ishonchliligi va jurnalist mehnat xavfsizligiga ta'sirini baholash hamda amaliy himoya modelini asoslashdir. Metodologiya sifatida kontent xavf auditi, hodisalar tahlili va solishtirma yondashuv qo'llanadi. Ilmiy yangilik sifatida tahririyat xavfsizligi uchun risk-matritsa va tekshiruv protokoli integratsiyasi taklif etiladi.
Kalit so'zlar. internet jurnalistika; kiberxavfsizlik; fact-checking; dezinformatsiya; ijtimoiy muhandislik; ma'lumotlarni shifrlash; tahririyat protokoli

Аннотация. В тезисе анализируется безопасность интернет-журналистики в контексте редакционных процессов, технологической инфраструктуры и взаимодействия с аудиторией. Цель исследования состоит в классификации цифровых угроз, оценке их влияния на достоверность информации и безопасность труда журналиста, а также в обосновании практической модели защиты. Методология включает аудит рисков контента, анализ инцидентов и сравнительный подход. Научная новизна заключается в предложении интеграции риск-матрицы и протокола верификации для редакционной безопасности.
Ключевые слова. интернет-журналистика; кибербезопасность; фактчекинг; дезинформация; социальная инженерия; шифрование данных; редакционный протокол

Abstract. This thesis examines internet journalism security through editorial workflows, technological infrastructure, and audience interaction. The study aims to classify digital threats, evaluate their impact on information reliability and journalists' occupational safety, and substantiate a practical protection model. Methodology combines content risk auditing, incident analysis, and comparative assessment. The scientific novelty lies in integrating a newsroom risk matrix with a verification protocol, enabling systematic mitigation of cyber, informational, and social-engineering risks in online media production.
Keywords. internet journalism; cybersecurity; fact-checking; disinformation; social engineering; data encryption; newsroom protocol.

Internet jurnalistika xavfsizligi tushunchasi raqamli muhitda axborotni yig'ish, qayta ishlash, e'lon qilish va tarqatish bosqichlarida yuzaga keladigan texnik, tashkiliy hamda psixologik xatarlarni boshqarish tizimi sifatida ta'riflanadi. Uning mexanizmi tahririyatning identifikatsiya va autentifikatsiya tartiblaridan tortib, manbani tekshirish, metama'lumotlarni himoyalash va auditoriya bilan muloqotdagi xavfsiz amaliyotlargacha bo'lgan uzluksiz jarayonlar zanjiridan iborat bo'ladi. Masalan, onlayn nashrda tezkor xabar tayyorlashda jurnalist Telegram yoki elektron pochta orqali kelgan "hujjat"ni tekshirmasdan e'lon qilsa, bu nafaqat dezinformatsiya, balki zararli fayl orqali tahririyat tarmog'iga kirish kabi

kiberhodisaga ham sabab bo‘lishi mumkin. Amaliy statistik kuzatuvlarda tahririyatlarda uchraydigan hodisalarning sezilarli qismi parolning zaifligi, qayta ishlatilishi va fishing orqali qo‘lga kiritilishi bilan bog‘lanishi qayd etiladi, chunki ko‘plab tashkilotlarda ikki omilli autentifikatsiya to‘liq joriy etilmaydi va bu riskni oshiradi [4]. Ilmiy izoh shundan iboratki, internet jurnalistikasi xavfsizligi faqat “kompyuter xavfsizligi” bilan cheklanmaydi, u axborotning epistemik sifatlari, tahririyat etikasi va texnik himoya o‘rtasidagi muvozanatni saqlashni talab qiladigan ko‘p qatlamli tizimdir [1].

Internet jurnalistikasida tahdidlar tasnifi, avvalo, axborot tahdidlari, kibertexnik tahdidlar va ijtimoiy-psixologik tahdidlar kabi uch yo‘nalishda ta’riflanadi. Mexanizm nuqtayi nazaridan axborot tahdidlari faktlarning buzib ko‘rsatilishi, kontekstdan uzib berilishi va manipulyativ sarlavhalar orqali auditoriya qaroriga ta’sir o‘tkazishdan iborat bo‘lsa, kibertexnik tahdidlar zararli dastur, DDoS, akkaunt o‘g‘irlash va ma’lumotlar sizib chiqishi orqali tahririyat resurslarini izdan chiqaradi; ijtimoiy-psixologik tahdidlar esa doxxing, ta’qib va reputatsion bosim orqali jurnalistni o‘zini o‘zi senzura qilishga majbur etadi. Masalan, “deepfake” texnologiyasi yordamida tayyorlangan soxta video ijtimoiy tarmoqlarda tarqalib, tahririyatni shoshma-shosharlik bilan izoh berishga undaydi va ayni vaqtda video manbasi yuborilgan havola zararli skript bo‘lishi ehtimoli ham mavjud. Raqamli amaliyotda soxta kontentning tarqalish tezligi ko‘pincha tuzatish va rad etish tezligidan yuqori bo‘lib, auditoriya diqqat iqtisodiyotida birinchi xabar ko‘proq iz qoldiradi; shu sababli tekshiruv protokollari vaqt bosimini kamaytiradigan tashkiliy yechim sifatida ko‘riladi [6]. Ilmiy izoh sifatida qayd etish lozimki, tahdidlar tasnifi risklarni o‘lchash va resurslarni taqsimlash uchun zarur bo‘lgan analitik asbobdir, chunki barcha xavflar bir xil ehtimollik va bir xil zarar ko‘lamiga ega emas [4].

Tahririyat ish jarayonida xavfsizlik madaniyati deganda xodimlarning bilim, ko‘nikma va institutsional odatlari yig‘indisi, ya’ni xavfsizlikni “bir martalik sozlama” emas, balki doimiy boshqariladigan amaliyot sifatida qabul qilishi ta’riflanadi. Uning mexanizmi xodimlarni muntazam o‘qitish, rollarga asoslangan kirish huquqlari, shubhali kontent bilan ishlash protokoli, zaxira nusxa va favqulodda tiklash rejalarini bir tizimga bog‘lash orqali ishlaydi. Masalan, tahririyatda “nolinchi ishonch” tamoyili joriy etilib, har bir yangi qurilma va har bir yangi kirish sessiyasi qayta tekshirilsa, ichki tarmoqka tasodifiy zararli ulanish ehtimoli kamayadi, shuningdek xodimlar shaxsiy qurilmalarini ish resurslariga ulamasdan oldin minimal talablarga rioya qiladi. Amaliy ko‘rsatkich sifatida, ko‘plab tashkilotlarda xavfsizlik hodisalari inson omili bilan bog‘liq bo‘lishi ilmiy adabiyotlarda muntazam ta’kidlanadi; bu, ayniqsa, ijtimoiy muhandislik usullarida “tezlik” va “shoshilinchlik” signallari orqali xodim psixologiyasiga ta’sir qilinishi bilan izohlanadi [2]. Ilmiy izoh shundan iboratki, xavfsizlik madaniyati tashkiliy immunitet vazifasini bajaradi: texnik himoya vositalari buzilishi mumkin, biroq to‘g‘ri protokol va reflekslar hodisa oqibatini chegaralashga yordam beradi [1].

Internet jurnalistikasida manbalarni himoyalash va anonimlikni ta’minlash masalasi jurnalistikaning ijtimoiy funksiyasi bilan bog‘liq bo‘lgan axloqiy va huquqiy majburiyat sifatida ta’riflanadi. Mexanizm jihatidan bu aloqa kanallarini shifrlash, metama’lumotlarni minimallashtirish, saqlash muddatlarini qisqartirish va manba identifikatorlarini ajratilgan muhitda yuritish orqali amalga oshiriladi. Masalan, tahririyat muhim mavzuda material tayyorlayotganda manba yuborgan faylning EXIF metama’lumotlari undagi joylashuv va qurilma identifikatorlarini oshkor qilishi mumkin, shu bois nashrga tayyorlashdan avval metama’lumotlarni tozalash va faylni ajratilgan kompyuterda tekshirish amaliyoti qo‘llanadi. Amaliy raqam sifatida shifrlash mexanizmlarida ko‘p uchraydigan algoritmlardan biri AES-256 bo‘lib, u simmetrik shifrlashning mustahkam sanoat standarti sifatida tan olinadi; shuningdek xesh tekshiruvida SHA-256 kabi funksiyalar fayl yaxlitligini tekshirishga xizmat qiladi va ularni protokolga kiritish jurnalistning ish jarayonini standartlashtiradi. Ilmiy izoh

shuki, shifrlash formulasi sifatida C = E(K, P) va P = D(K, C) ko‘rinishidagi munosabat (bu yerda P ochiq matn, C shifrmatn, K kalit) axborotning maxfiyligi bilan birga kalitlarni boshqarish muammosini ham keltirib chiqaradi, ya’ni xavfsizlik faqat algoritm kuchida emas, kalitlar hayotiy siklini boshqarish sifatida namoyon bo‘ladi [4].

Dezinformatsiya va verifikatsiya muammosi internet jurnalistikasi xavfsizligining epistemik, ya’ni bilimning ishonchliligiga daxldor qismi sifatida ta’riflanadi. Mexanizm sifatida fakt-cheking, triangulyatsiya, ochiq manbalar razvedkasi va tahririyat ichki “ikki bosqichli tasdiq” tamoyili ishlaydi, bunda har bir muhim da’vo kamida ikki mustaqil ishonchli manbadan tasdiqlanmaguncha nashr etilmaydi. Masalan, ijtimoiy tarmoqda tarqalgan surat bo‘yicha tahririyat geolokatsiya, vaqt belgisi, soyalar va ob-havo ma’lumotlarini solishtirib, rasmning haqiqiyligi hamda voqea joyini aniqlashga urinadi, so‘ngra rasmning oldin e’lon qilingan-yo‘qligini teskari qidiruv orqali tekshiradi. Amaliy kuzatuv shuni ko‘rsatadiki, onlayn platformalarda noto‘g‘ri axborotning “ko‘rinishi” ko‘pincha algoritmik tavsiyalar sabab kuchayadi va bu tahririyatdan tezkorlik bilan birga metodik ehtiyotkorlikni talab qiladi; shu bois verifikatsiya protokoli vaqtni tejaydigan chek-listlar emas, balki ishonchlilikni o‘lchash mezonlari bilan boyitilgan jarayon bo‘lishi lozim [6]. Ilmiy izoh nuqtayi nazaridan, verifikatsiya jarayoni informatsion xavfsizlikning “yaxlitlik” komponentiga to‘g‘ridan-to‘g‘ri mos keladi, chunki axborotning o‘zgartirilmaganligi va kontekstga mosligi ta’minlanmasa, maxfiylik va mavjudlikning o‘zi jurnalistik qiymatni kafolatlamaydi [2].

Tahririyat uchun risklarni baholash modeli internet jurnalistikasi xavfsizligini boshqaruv qarorlariga aylantiradigan analitik vosita sifatida ta’riflanadi. Mexanizm sifatida risk ehtimolligi va ta’sir kuchi ko‘paytmasiga asoslangan matritsa, aktivlar ro‘yxati, tahdid aktorlari profili va nazorat choralari (controls) katalogi qo‘llanadi, bunda har bir aktiv uchun minimal zarur himoya darajasi belgilanadi. Masalan, tahririyatning asosiy aktivlari sifatida domen va DNS boshqaruvi, CMS administrator akkaunti, jurnalistlarning pochta qutilari, manbalar arxivi va mobil qurilmalar ko‘rilib, har biri bo‘yicha “kirish yo‘llari” va “eng yomon stsenariy” hujjatlashtiriladi. Amaliy jadval ko‘rinishida quyidagi soddalashtirilgan risk-matritsa tahririyat ehtiyojlari uchun moslashtiriladi, unda ballar 1 dan 5 gacha o‘lchanadi va ustuvorlik aniqlanadi; bunday ballash resursi cheklangan sharoitda qaysi choralar birinchi navbatda joriy etilishini belgilashga yordam beradi.

Jadval. Tahririyat risk-matritsasi (soddalashtirilgan)

Aktiv: CMS admin akkaunti. Tahdid: fishing orqali parol o‘g‘irlash. Ehtimollik: 4. Ta’sir: 5. Risk balli: 20. Nazorat: 2FA; parol menejeri; kirish jurnali.

Aktiv: Manbalar arxivi. Tahdid: sizib chiqish. Ehtimollik: 3. Ta’sir: 5. Risk balli: 15. Nazorat: shifrlash; segmentatsiya; minimal kirish.

Aktiv: Sayt mavjudligi. Tahdid: DDoS. Ehtimollik: 3. Ta’sir: 4. Risk balli: 12. Nazorat: CDN; WAF; trafik filtri.

Aktiv: Jurnalist mobil qurilmasi. Tahdid: yo‘qotish yoki o‘g‘irlanish. Ehtimollik: 4. Ta’sir: 3. Risk balli: 12. Nazorat: ekran qulfi; masofaviy o‘chirish; zaxira.

Ilmiy izoh shundan iboratki, risk-matritsa metodologiyasi texnik va ijtimoiy tahdidlarni bir o‘lchov maydoniga keltirib, tahririyatning strategik rejalashtirishiga moslashtiradi, ammo u doimiy ravishda hodisalar tahlili bilan yangilanmasa, tez eskiruvchi raqamli muhitda real holatni aks ettirmay qoladi [4]. Shu sababli risklarni baholashda solishtirma yondashuv ham muhim bo‘lib, ya’ni OAVning o‘lchami, auditoriya miqyosi va kontent yo‘nalishiga qarab nazorat choralari darajasi farqlanadi, chunki “bir xil himoya hamma uchun” tamoyili amalda samarasiz bo‘lishi mumkin [1]. Misol sifatida, kichik tahririyatda alohida xavfsizlik bo‘limi bo‘lmasligi mumkin, lekin minimal protokollar va avtomatlashtirilgan yangilanishlar orqali riskning asosiy qismi pasaytiriladi; yirik media tashkilotda esa SIEM, kirish auditlari va segmentatsiya kabi murakkab tizimlar zarur bo‘ladi. Amaliy statistika sifatida, hodisalarga

javob berish va tiklashga sarflanadigan vaqtning qisqarishi ko‘pincha oldindan tayyorlangan “incident response” rejasiga bog‘liq bo‘lib, reja mavjud bo‘lmagan holatda tiklanish cho‘zilishi va reputatsion zarar ortishi ilmiy manbalarda asoslanadi [2]. Ilmiy izoh yakunida aytish joizki, risk-boshqaruv modeli internet jurnalistikasida xavfsizlikni texnik “vosita”dan tashkiliy “institut”ga aylantiradi, bu esa 10.00.09 ixtisosligi doirasida media jarayonlarining barqarorligini ta’minlashga xizmat qiladi.

Xulosa qismida internet jurnalistika xavfsizligi raqamli muhitda axborotning maxfiyligi, yaxlitligi va mavjudligini ta’minlash bilan birga, jurnalistik ishonchlilik va mehnat xavfsizligini ham qamrab oladigan kompleks hodisa ekani umumlashtiriladi. Tadqiqotda tahdidlarning uch yo‘nalishli tasnifi, xavfsizlik madaniyati va manbani himoyalash amaliyotlari bir-biri bilan uzviy bog‘langanligi, shuningdek dezinformatsiyaga qarshi verifikatsiya jarayoni axborot xavfsizligining markaziy tarkibiy qismi ekani sintez qilindi. Taklif etilgan risk-matritsa va tekshiruv protokoli integratsiyasi tahririyat resurslari cheklangan sharoitda ham ustuvor choralarni aniqlash, hodisalarni oldini olish hamda oqibatlarni minimallashtirish imkonini beradi. Natijada internet jurnalistikasida xavfsizlikni boshqarish texnik vositalar, tashkiliy reglamentlar va jurnalistik metodologiya birikmasi sifatida qaralishi lozimligi asoslandi. Kelgusida ushbu yondashuvni mahalliy tahririyatlar amaliyotiga mos indikatorlar orqali o‘lchash va trening modullarini standartlashtirish ilmiy-amaliy samaradorlikni oshiradi.

Foydalanilgan adabiyotlar ro‘yxati

1. McQuail D. McQuail’s Mass Communication Theory. London: SAGE Publications, 2010. 632 p.
2. Mitnick K. D., Simon W. L. The Art of Deception: Controlling the Human Element of Security. Indianapolis: Wiley Publishing, 2002. 368 p.
3. Kovach B., Rosenstiel T. The Elements of Journalism: What Newspeople Should Know and the Public Should Expect. New York: Three Rivers Press, 2007. 384 p.
4. Stallings W., Brown L. Computer Security: Principles and Practice. Boston: Pearson, 2018. 816 p.
5. Дзялошинский И. М. Социальные коммуникации и журналистика: теория и практика. Москва: Аспект Пресс, 2010. 352 с.
6. Karimov I. A. Internet jurnalistikasi: nazariya va amaliyot. Toshkent: O‘zbekiston, 2019. 240 b.