

MEDIA AXBOROT XAVFSIZLIGI SOHASIDA MAVJUD MUAMMOLARNING INTEGRATIV TAHLILI

Anvarova Muqaddas Xomidjon qizi

O'zbekiston jurnalistika va ommaviy kommunikatsiyalar universiteti

Xalqaro jurnalistika yo'nalishi 3- kurs talabasi

Annotatsiya: Noto'g'ri ma'lumot va dezinformatsiya ommaviy axborot vositalarining axborot xavfsizligi uchun jiddiy muammolarni keltirib chiqaradi. Noto'g'ri ma'lumot yomon niyatsiz tarqatilgan yolg'on yoki chalg'ituvchi ma'lumotni anglatadi, dezinformatsiya esa aldash va manipulyatsiya qilish uchun ataylab uydiriladi. Ijtimoiy tarmoqlarning o'sishi ikkalasining ham tarqalishini kuchaytirdi, bu ishonchli manbalarni ishonchsiz manbalardan ajratishni qiyinlashtirdi. Soxta xabarlar, deepfakes va aniq suratlar ommaviy axborot vositalariga bo'lgan ishonchni yo'qotib, yolg'on ma'lumot tarqatish uchun ishlatiladigan vositalardan biridir.

Kalit so'zlar: Yolg'on axborot, dezinformatsiya, Ijtimoiy tarmoq, integrativ tahlil

Axborot-kommunikatsiya texnologiyalarining keng tarqalishi axborotni iste'mol qilish, almashish va saqlash usullarini o'zgartirgan bugungi raqamli asrda ommaviy axborot vositalarining axborot xavfsizligi muhim muammo hisoblanadi. Internet va ijtimoiy tarmoqlarning paydo bo'lishi ma'lumot tarqatishni demokratlashtirdi, ammo xavfsizlikka oid ko'plab muammolarni keltirib chiqardi. Kibertahdidlar yanada murakkablashib, keng tarqalib borayotganligi sababli, ommaviy axborot vositalari ma'lumotlarining yaxlitligi, maxfiyligi va mavjudligini ta'minlash muhim ahamiyatga ega bo'ldi. Ushbu integratsion tahlil kiberhujumlar, noto'g'ri ma'lumotlar va dezinformatsiyalar, maxfiylik muammolari, tartibga solish muammolari va rivojlanayotgan texnologiyalarning roli kabi asosiy masalalarga e'tibor qaratib, ommaviy axborot vositalarining axborot xavfsizligi sohasidagi mavjud muammolarni o'rganadi¹.

Ommaviy axborot vositalarining axborot xavfsizligini ta'minlashning eng dolzarb muammolaridan biri bu kiberhujumlarning keng tarqalishidir. Ushbu hujumlar turli shakllarda bo'lishi mumkin, jumladan, fishing, zararli dastur, to'lov dasturi va tarqatilgan xizmatni rad etish (DDoS) hujumlari. Ommaviy axborot vositalari kiberjinoyatchilarning asosiy maqsadi bo'lib, ular o'zlari ishlayotgan ma'lumotlarning yuqori qiymati hisoblanadi. Masalan, 2014-yilgi Sony Pictures-ning buzib kirishi nozik ma'lumotlarni oshkor qildi va bunday buzilishlar media kompaniyalariga qanday

¹ Herath, T., Khanna, P., & Ahmed, M. (2022). Cybersecurity Practices for Social Media Users: A Systematic Literature Review. *Journal Of Cybersecurity and Privacy*, 2(1), 1-18

dahshatli ta'sir ko'rsatishi mumkinligini ta'kidladi. Xuddi shunday, 2017-yilgi WannaCry ransomware hujumi butun dunyo bo'ylab ko'plab tashkilotlarga, jumladan, ommaviy axborot vositalariga ta'sir ko'rsatib, operatsiyalarni to'xtatib, katta moliyaviy yo'qotishlarga olib keldi.

Jismoniy shaxslar va korxonalar tomonidan Facebook, Twitter va Instagram kabi ijtimoiy media platformalaridan keng foydalanish kiberxavfsizlik tahdidlarining mos ravishda oshishiga olib keldi. Ushbu platformalar, aloqa va o'zaro bog'lanish uchun kuchli vositalar bo'lsa-da, kiber jinoyatchilar foydalanishni xohlaydigan ko'plab zaifliklarni o'z ichiga oladi. Har kuni millionlab foydalanuvchilar shaxsiy va nozik ma'lumotlarni almashishi bilan kiberhujumlar xavfi doimo mavjud.

Fishing ijtimoiy tarmoqlardagi eng keng tarqalgan va xavfli tahdidlardan biri bo'lib qolmoqda. Kiberjinoyatchilar ishonchli manbalardan kelgan aldamchi elektron pochta va xabarlarni tayyorlab, foydalanuvchilarni parollar va kredit karta ma'lumotlari kabi nozik ma'lumotlarni oshkor qilishga undaydi. Ushbu hujumlar ko'pincha shoshilinch so'rovlar yoki jozibador takliflar sifatida yashirinib, ularni tanib olishni qiyinlashtiradi.

Kiberjinoyatchilar, shuningdek, zararli dasturlar va to'lov dasturlarini tarqatish uchun ijtimoiy tarmoqlardan foydalanadilar. Zararli havolalarni bosish yoki virusli fayllarni yuklab olish uchun foydalanuvchilarni aldab, tajovuzkorlar muhim ma'lumotlarni shifrlaydigan dasturiy ta'minotni o'rnatishi va ularni chiqarish uchun to'lov talab qilishi mumkin. Ushbu turdagi hujum, ayniqsa, kasalxonalar kabi muassasalar uchun zararli bo'lib, bu yerda ma'lumotlarga kirish bemorlarni parvarish qilish va operatsiyaning uzluksizligi uchun juda muhimdir².

Media tashkilotlariga kiberhujumlar maxfiy ma'lumotlarning o'g'irlanishi, xizmatlarning uzilishi va obro'siga putur yetkazishi mumkin. Media axborot tizimlaridagi zaifliklar ko'pincha eskirgan dasturiy ta'minot, yetarli darajada xavfsizlik choralari va xodimlarning kiberxavfsizlik bo'yicha xabardorligi yo'qligidan kelib chiqadi. Kibertahdidlar rivojlanishda davom etar ekan, media tashkilotlari kiberxavfsizlikning mustahkam amaliyotlarini, jumladan dasturiy ta'minotni muntazam yangilash, xodimlarni o'qitish va tajovuzlarni aniqlash tizimlari va shifrlash kabi ilg'or xavfsizlik texnologiyalarini joriy etishlari kerak.

Noto'g'ri ma'lumot va dezinformatsiya ommaviy axborot vositalarining axborot xavfsizligi uchun jiddiy muammolarni keltirib chiqaradi. Noto'g'ri ma'lumot yomon niyatsiz tarqatilgan yolg'on yoki chalg'ituvchi ma'lumotni anglatadi, dezinformatsiya esa aldash va manipulyatsiya qilish uchun ataylab uydiriladi. Ijtimoiy tarmoqlarning o'sishi ikkalasining ham tarqalishini kuchaytirdi, bu ishonchli manbalarni ishonchsiz manbalardan ajratishni qiyinlashtirdi. Soxta xabarlar, deepfakes va aniq suratlar

² Khan, N., Ikram, N., Murtaza, H., & Asadi, M. (2021). Social media users and cybersecurity awareness: predicting self-disclosure using a hybrid artificial intelligence approach

ommaviy axborot vositalariga bo'lgan ishonchni yo'qotib, yolg'on ma'lumot tarqatish uchun ishlatiladigan vositalardan biridir.

Noto'g'ri ma'lumot va dezinformatsiyaning oqibatlari juda keng bo'lishi mumkin. Ular jamoatchilik fikriga ta'sir qilishi, saylov natijalariga ta'sir qilishi, zo'ravonlikni qo'zg'atishi va demokratik jarayonlarga putur yetkazishi mumkin. Misol uchun, 2016-yilgi AQSh prezidentlik saylovlari paytida noto'g'ri ma'lumotlarning tarqalishi chet el aralashuvi va ijtimoiy medianing siyosiy rivoyatlarni shakllantirishdagi roli haqida tashvish uyg'otdi. Ushbu muammolarga qarshi kurashish uchun media tashkilotlari va texnologiya kompaniyalari faktlarni tekshirish tashabbuslariga sarmoya kiritishlari, soxta yangiliklarni aniqlash algoritmlarini ishlab chiqishlari va jamoatchilik orasida mediasavodxonlikni oshirishlari kerak.

Jahon Iqtisodiy Forumining 2013-yilgi Global Risklar hisoboti qurolli ijtimoiy media saytlari va kiber urushda noto'g'ri ma'lumotlardan strategik foydalanish xavfini ta'kidladi. Ijtimoiy media platformalari ma'lumotlarni oson almashish uchun mo'ljallangan, afsuski, bu ularni maxfiylik buzilishi va ma'lumotlar sizib chiqishiga moyil qiladi. Foydalanuvchilar ko'pincha potensial xavflarni sezmasdan shaxsiy ma'lumotlarini baham ko'rishadi, bu ularni shaxsiy ma'lumotlarni o'g'irlash va kiberjinoyatning boshqa shakllariga qarshi himoyasiz qiladi. LinkedIn kabi platformalar kiberjinoyatchilarni maqsadli hujumlar uchun ko'plab ma'lumotlar bilan ta'minlab, katta ma'lumotlar buzilishini ko'rdi³.

Korporatsiyalar uchun ijtimoiy tarmoqlarning axborot tarqatish kuchi dilemma tug'diradi. Bir tomondan, bu katta auditoriya bilan samarali muloqot qilish va jalb qilish imkonini beradi. Boshqa tomondan, bu maxfiy ma'lumotlarni himoya qilish vazifasi yuklangan xavfsizlik guruhlari va kibermutaxassislar uchun qiyinchiliklar tug'diradi.

Kiberjinoyatchilar fishing elektron pochta xabarlari va zararli dasturlarni o'rnatish kabi murakkab taktikalar orqali jismoniy shaxslar va tashkilotlarni tobora ko'proq nishonga olishmoqda. Ushbu zararli harakatlar ko'pincha buzilgan yoki ekspluatatsiya qilingan veb-saytlardan kelib chiqadi. Kiberhujumlarning eng makkor shakllaridan biri bu to'lov dasturi bo'lib, u muhim ma'lumotlarni shifrlaydi, dasturiy ta'minotga zarar yetkazadi va shifrnı ochish kaliti uchun to'lovni talab qiluvchi tovlamachilik xabarlarini ko'rsatadi. Bu, ayniqsa, ma'lumotlarga doimiy kirish bemorlarni parvarish qilish va operatsion samaradorlik uchun juda muhim bo'lgan shifoxonalar va parvarishlash muassasalari uchun halokatli. To'lov talablari sezilarli darajada farq qilishi mumkin, bu maqsadli sub'ektlarga qo'shimcha moliyaviy qiyinchiliklarni keltirib chiqaradi⁴.

³ Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, 64(5), 659-671.

⁴ Snider, K., Shandler, R., Zandani, S., & Canetti, D. Cyberattacks, cyber threats, and attitudes toward cybersecurity policies. *Journal Of Cybersecurity*, 7(1). 2021. P.67.

Mashhurlik va reklama daromadi uchun foydalanuvchi tomonidan yaratilgan kontentga (UGC) tayanish ijtimoiy media platformalarini kiberhujumlarga ayniqsa sezgir qiladi. UGC ko'pincha xakerlar tomonidan ishlatilishi mumkin bo'lgan nozik ma'lumotlarni o'z ichiga oladi. Foydalanuvchilarning hissasiga tayanish nafaqat platformalarning potentsial buzilishlarga ta'sirini oshiradi, balki ma'lumotlar xavfsizligini ta'minlash vazifasini ham murakkablashtiradi. Ijtimoiy tarmoqlardan foydalanishga xos bo'lgan tez-tez yangilanishlar va o'zaro ta'sirlar kiberjinoyatchilarga hujumlar uyushtirish va ma'lumotlarni o'g'irlash uchun ko'plab imkoniyatlarni taqdim etadi.

Ushbu o'sib borayotgan tahdidlarga javoban, ko'plab kompaniyalar o'zlarining xavfsizligini oshirish va foydalanuvchilarning ma'lumotlarini himoya qilish uchun faol choralar ko'rmoqda. Ba'zilar foydalanuvchilarga xavfsizlik sozlamalarini kuzatishga va hisoblarini suiiste'mol qilishdan himoya qilishga yordam beradigan o'ziga xos xususiyatlarni joriy qilgan. Misol uchun, ko'p faktorli autentifikatsiya (MFA) va ilg'or shifrlash usullari ko'plab platformalarda standart xususiyatlarga aylanmoqda. Bundan tashqari, kompaniyalar onlayn firibgarlik haqida xabardorlikni oshirish va foydalanuvchilarga Internetda xavfsiz qolish bo'yicha amaliy maslahatlar berish uchun ta'lim kampaniyalarini boshlaydi.

Ransomware so'nggi yillarda sezilarli o'sish kuzatilgan kiberjinoyatlarning ayniqsa halokatli shaklidir. Kiber o'g'rilar hayotiy ma'lumotlarni shifrlash uchun to'lov dasturini o'rnatadilar va to'lov to'lanmaguncha ularga kirish imkoni bo'lmaydi. Ushbu turdagi hujum, ayniqsa, shifxonalar va sog'liqni saqlash muassasalari kabi doimiy ma'lumotlardan foydalanishga tayanadigan muassasalar uchun zararli. Ransomware hujumining ta'siri halokatli bo'lishi mumkin, bu muhim xizmatlarni buzishi va hayotni xavf ostiga qo'yishi mumkin. To'lov dasturining moliyaviy talablari ham juda munozarali bo'lishi mumkin, to'lov miqdori maqsad va shifrlangan ma'lumotlarning qabul qilingan qiymatiga qarab keng farq qiladi.

Texnologiyalardagi yutuqlar kiberxavfsizlik sohasida ham imkoniyatlar, ham muammolarni taqdim etdi. Maxfiylik va ishonch masalalarini yaxshi bilmasligi mumkin bo'lgan ijtimoiy media foydalanuvchilariga qaratilgan takomillashtirilgan texnologiyalar va murakkab strategiyalar ishlab chiqilmoqda. Ushbu yutuqlar real vaqt rejimida kiber tahdidlarni aniqlash va kamaytirish uchun sun'iy intellektdan (AI) foydalanishni, shuningdek ma'lumotlar xavfsizligi va yaxlitligini oshirish uchun blokcheyn texnologiyasini o'z ichiga oladi⁵.

Sun'iy intellekt (AI), blokcheyn va narsalar interneti (IoT) kabi rivojlanayotgan texnologiyalar ommaviy axborot vositalarining axborot xavfsizligi uchun ham imkoniyatlar, ham muammolarni taqdim etadi. AI va mashinani o'rganish

⁵ van der Walt, E., Eloff, J., & Grobler, J. Cyber-security: Identity deception detection on social media platforms. Computers & Security. 2018. P.76-79.

anomaliyalarni aniqlash va potentsial tahdidlarni bashorat qilish orqali kiberxavfsizlikni oshirishi mumkin. Misol uchun, AI algoritmlari kiberhujumlarni ko'rsatadigan naqshlarni aniqlash uchun katta hajmdagi ma'lumotlarni tahlil qilishi mumkin, bu esa buzilishlarning oldini olish uchun faol choralar ko'rish imkonini beradi.

Biroq, bu texnologiyalar kiber jinoyatchilar tomonidan ham qo'llanilishi mumkin. Masalan, sun'iy intellekt yordamida ishlaydigan deepfakes media ma'lumotlarining yaxlitligiga jiddiy tahdid soladigan, aniqlash qiyin bo'lgan real, ammo soxta videolarni yaratishi mumkin. Xuddi shunday, IoT qurilmalarining ko'payishi kiberjinoyatchilar uchun hujum maydonini oshiradi, chunki bu qurilmalarning aksariyatida tegishli xavfsizlik choralari mavjud emas.

Blokcheyn texnologiyasi media axborot xavfsizligini oshirish uchun potentsial echimlarni taklif qiladi. Uning markazlashtirilmagan va o'zgarmas tabiati kiberjinoyatchilarga axborotni o'zgartirishni qiyinlashtiradi, bu esa media-kontentning haqiqiylikni tekshirishning xavfsiz usulini ta'minlaydi. Blockchain, shuningdek, kontentga egalik haqidagi shaffof va buzg'unchilikka qarshi yozuvlarni ta'minlash orqali xavfsiz tranzaksiyalarni amalga oshirishi va intellektual mulk huquqlarini himoya qilishi mumkin.

Maxfiylik masalalari ommaviy axborot vositalarining axborot xavfsizligidagi yana bir muhim muammodir. Media tashkilotlari tomonidan shaxsiy ma'lumotlarni to'plash, saqlash va tarqatish, agar to'g'ri boshqarilmasa, shaxsiy hayotning buzilishiga olib kelishi mumkin. Facebook-Cambridge Analytica mojarosi kabi shov-shuvli holatlar shaxsiy ma'lumotlardan foydalanuvchilarning roziligisiz siyosiy va tijorat maqsadlarida qanday foydalanish mumkinligini ta'kidladi. Bunday hodisalar ma'lumotlarni himoya qilish qoidalarini kuchaytirish va ommaviy axborot vositalarining shaxsiy ma'lumotlar bilan qanday ishlashini tekshirishni kuchaytirish talablarini keltirib chiqardi.

Media tashkilotlari foydalanuvchilarning shaxsiy hayotini himoya qilish uchun ma'lumotlarni himoya qilish bo'yicha keng qamrovli choralar ko'rishlari kerak. Bunga ma'lumotlarni shifrlashni amalga oshirish, shaxsiy ma'lumotlarni anonimlashtirish va Yevropa Ittifoqida ma'lumotlarni himoya qilish bo'yicha umumiy reglament (GDPR) kabi ma'lumotlarni himoya qilish qoidalariga rioya qilishni ta'minlash kiradi. Bundan tashqari, tashkilotlar ma'lumotlarni to'plash amaliyoti bo'yicha shaffof bo'lishi va foydalanuvchilarga shaxsiy ma'lumotlarini nazorat qilishni ta'minlashi kerak.

Ommaviy axborot vositalarining axborot xavfsizligini tartibga soluvchi landshaft murakkab va turli yurisdiksiyalarda farqlanadi. Ba'zi mamlakatlarda ma'lumotlarni himoya qilish bo'yicha qat'iy qonunlar mavjud bo'lsa-da, boshqalarida rivojlanayotgan kiber tahdid landshaftini hal qilish uchun keng qamrovli qoidalar yo'q. Ushbu nomuvofiqlik bir nechta mintaqalarda faoliyat yurituvchi media tashkilotlari uchun

qiyinchiliklar tug'diradi, chunki ular turli qonuniy talablarni bajarishi va mahalliy qoidalarga rioya etilishini ta'minlashi kerak.

Normativ muammolar mavjud qonunlarning bajarilishiga ham taalluqlidir. Cheklangan resurslar, yurisdiksiya muammolari va texnologik taraqqiyotning tez sur'atlari nazorat qiluvchi organlarning paydo bo'ladigan tahdidlarga mos kelishini qiyinlashtiradi. Ushbu muammolarni hal qilish uchun xalqaro hamkorlik va me'yoriy hujjatlarni uyg'unlashtirish zarur. Ommaviy axborot vositalarining axborot xavfsizligi bo'yicha global standartlarni o'rnatish chegaralar bo'ylab axborotni himoya qilishda izchil va ishonchli yondashuvni ta'minlashga yordam beradi.

Ogohlik va ta'lim kibertahdidlarga qarshi kurashning muhim tarkibiy qismidir. Ko'pgina kiberxavfsizlik buzilishlari foydalanuvchilar o'rtasida bilim va xabardorlikning yetishmasligi tufayli yuzaga keladi. Foydalanuvchilarni fishing, zararli dasturlar va boshqa kiber tahdidlar haqida ma'lumot berish juda muhim. Xavfsiz ko'rish amaliyotlari, kuchli parollarning ahamiyati va shaxsiy ma'lumotlarni onlayn almashish xavfini ta'kidlaydigan ta'lim kampaniyalari kiberjinoyatlar sonini sezilarli darajada kamaytirishi mumkin⁶.

Ommaviy axborot vositalarining axborot xavfsizligi sohasidagi mavjud muammolarni hal qilish uchun ko'p qirrali yondashuv talab etiladi. Bunga texnologik yechimlar, me'yoriy-huquqiy bazalar va manfaatdor tomonlarning hamkorlikdagi harakatlari kiradi.

- Texnologik yechimlar: OAV tashkilotlari o'zlarining axborot tizimlarini himoya qilish uchun ilg'or kiberxavfsizlik texnologiyalariga sarmoya kiritishlari kerak. Bunga ko'p faktorli autentifikatsiya, shifrlash va hujumlarni aniqlash tizimlarini joriy etish kiradi. Bundan tashqari, AI va mashinani o'rganish tahdidlarni aniqlash va javob berish imkoniyatlarini yaxshilash uchun ishlatilishi mumkin.

- Normativ asoslar: Hukumatlar va tartibga soluvchi organlar rivojlanayotgan kibertahdid manzarasini hal qilish uchun keng qamrovli va uyg'unlashtirilgan qoidalarni ishlab chiqishlari kerak. Bunga ma'lumotlarni himoya qilish qonunlarini tatbiq etish, ma'lumotlarni yig'ish amaliyotida shaffoflikni ta'minlash va ommaviy axborot vositalarining axborot xavfsizligi bo'yicha global standartlarni o'rnatish kiradi.

- Hamkorlik va xabardorlik: Media tashkilotlari, texnologiya kompaniyalari va nazorat qiluvchi organlar o'rtasidagi hamkorlik kibertahdidlar va noto'g'ri ma'lumotlarga qarshi kurashda muhim ahamiyatga ega. Tahdid haqidagi ma'lumotlar va ilg'or tajribalarni almashish jamoaviy xavfsizlikni yaxshilashga yordam beradi. Bundan tashqari, ommaviy axborot vositalaridan savodxonlik va kiberxavfsizlik

⁶ Thakur, K., Hayajneh, T., & Tseng, J. Cyber Security in social media: Challenges and the Way Forward. IT Professional, 2019. P.41-49

haqida xabardorlikni oshirish noto'g'ri ma'lumotlarning ta'sirini yumshatish va umumiy xavfsizlikni kuchaytirish uchun juda muhimdir.

• Ta'lim: Media tashkilotlarida xodimlar uchun doimiy trening va ta'lim ularning so'nggi kiber tahdidlar va xavfsizlik amaliyotlaridan xabardor bo'lishini ta'minlash uchun juda muhimdir. Muntazam o'quv mashg'ulotlari, seminarlar va simulyatsiya qilingan kiberhujum ssenariylari xavfsizlikdan xabardorlik madaniyatini shakllantirishga yordam beradi.

• Tadqiqot va innovatsiyalar: Doimiy tadqiqot va innovatsiyalar paydo bo'ladigan tahdidlardan oldinda bo'lish uchun zarurdir. Ommaviy axborot vositalarining axborot xavfsizligini oshirish uchun yangi texnologiyalar va strategiyalarni ishlab chiqish uchun OAV tashkilotlari akademik institutlar va kiberxavfsizlik bo'yicha mutaxassislar bilan hamkorlik qilishi kerak.

Bugungi kunda ijtimoiy tarmoqlar orqali yuzaga kelayotgan yana bir jiddiy muammo bu ijtimoiy tarmoqlar orqali xalqaro terroristic guruhlar faoliyati hisoblanadi. Hozirgi dunyo shundayki, ochiq harbiy qarama-qarshilik va sovuq urushdan o'tib, xalqaro "birgalikda yashash" yangi davrga - axborot urushlari davriga kirmoqda. An'anaviy qurollardan farqli o'laroq, axborot makonidagi qarshi choralar tinchlik davrida samarali qo'llanilishi mumkin. Bu mablag'larning muhim xususiyati shundaki, ular nafaqat hukumat, balki terroristik va jinoiy tuzilmalar, shuningdek, jismoniy shaxslar uchun ham mavjud.

Axborot-telekommunikatsiya inqilobi sharoitida jamiyatning o'zgarishi kompyuter tarmoqlarida terrorchilik faoliyati uchun zamin yaratadi. Ijtimoiy tarmoqlaria jinoyatchilikning o'sishiga ta'sir qiluvchi ba'zi omillar:

- jamiyat hayotining barcha sohalarini global axborotlashtirish o'smaydi, balki uning xavfsizlik darajasini pasaytiradi;

- ilmiy-texnikaviy taraqqiyotning jadallashishi terrorchilarning sof tinch texnologiyalarni yo'q qilish vositasi sifatida foydalanish ehtimolini oshiradi va ulardan "ikki tomonlama" foydalanish imkoniyati ko'pincha nafaqat oldindan aytib bo'lmaydi, balki texnologiyani yaratuvchilar tomonidan ham amalga oshirilmaydi;

– terrorizm axborot texnologiyalarining alohida turiga aylanib bormoqda, chunki, birinchidan, terrorchilar aloqa va axborot to'plash uchun zamonaviy axborot va telekommunikatsiya tizimlari imkoniyatlaridan tobora ko'proq foydalanmoqda; ikkinchidan, "kiberterrorizm" deb ataladigan narsa bugungi kun haqiqatiga aylanib bormoqda, uchinchidan, aksariyat terroristik harakatlar nafaqat moddiy zarar etkazish, odamlarning hayoti va sog'lig'iga tahdid solishi, balki axborot va psixologik zarba berishga qaratilgan; uning ta'siri katta xalq ommasiga terrorchilar uchun o'z maqsadlariga erishish uchun qulay muhit yaratadi⁷;

⁷ Neumann, P. Options and Strategies for Countering Online Radicalization in the United States. Studies in Conflict & Terrorism. 2013. P.79.

– “raqamli tengsizlik” va axborot poygasida “yo‘qotgan” mamlakatlarning paydo bo‘lishi alohida davlatlarga qarshi terrorchilik faoliyati uchun sabab, assimetrik javob vositasi sifatida xizmat qilishi mumkin.

Davlat milliy xavfsizligining muhim tarkibiy qismlaridan biri sifatida axborot xavfsizligini ta‘minlash masalasi transmilliy (transchegaraviy) kompyuter jinoyati va kiberterrorizmning paydo bo‘lishi sharoitida ayniqsa keskinlashdi. Kiberhujumlar tahdidi juda real va u bilan bog‘liq xavflar mutaxassislar tomonidan yuqori darajada baholanmoqda.

Foydalanilgan adabiyotlar:

1. Kim, J., Malaiya, Y., Ray, I., 2007. Vulnerability Discovery in Multi-Version Software Systems. In: Cukic, B., Dong, J. (Eds.), Proceedings of the Tenth IEEE High Assurance Systems Engineering Symposium. IEEE Computer Society, November 14-16, Dallas, Texas, USA, pp. 141–148.
2. Le Roux N., Bengio Y. Representational power of restricted Boltzmann machines and deep belief networks // Neural computation. 2008. Vol. 20. No 6. P. 1631-1649.
3. Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. Business Horizons, 64(5), 659-671.
4. Mastoianni, B. (2015). Could Policing Social Media Help Prevent Terrorist Attacks? CBS News, 15 December. Retrieved 20 November 2017,
5. Mengersen K. Marin, J.M. and C.P. Robert. 2005. Bayesian modelling and inference on mixtures of distributions. Handbook of statistics (2005).
6. Nandanwar, R. (2013). Case Study of Recent Examples of Cyber Crime and E-Commerce Fraud related Investigations involving IPR and Copyright Act.