



Peculiarities of detecting traces of extortion committed via the Internet

Dilrabo TOPILDIYEVA¹

Tashkent State University of Law

ARTICLE INFO

Article history:

Received July 2024
Received in revised form
15 July 2024
Accepted 25 July 2024
Available online
15 August 2024

Keywords:

crime,
extortion,
the Internet,
traces,
detection,
virtual traces,
virtual space,
social networks,
cache files.

ABSTRACT

The article analyzes the types of traces in extortion committed on the Internet, issues of their detection and receipt.

2181-1415/© 2024 in Science LLC.

DOI: <https://doi.org/10.47689/2181-1415-vol5-iss7/S-pp278-282>

This is an open access article under the Attribution 4.0 International (CC BY 4.0) license (<https://creativecommons.org/licenses/by/4.0/deed.ru>)

Internet tovlamachiligi jinoyati bo'yicha izlarni aniqlashning o'ziga xos xususiyatlari

Kalit so'zlar:

jinoyat,
tovlamachilik,
internet,
izlar,
aniqlash,
virtual izlar,
virtual makon,
ijtimoiy tarmoqlar,
kesh fayllar.

ANNOTATSIYA

Maqolada internet tarmog'ida sodir etiladigan tovlamachilik jinoyatlari bo'yicha izlarning turlari, ularni aniqlash va olish masalalari tahlil etilgan.

¹ Senior Lecturer, Tashkent State University of Law, Tashkent, Uzbekistan. E-mail: d.topildieva@gmail.com

Особенности выявления следов при вымогательствах, совершенных через сети интернет

АННОТАЦИЯ

Ключевые слова:

преступление,
вымогательство,
интернет,
следы,
выявление,
виртуальные следы,
виртуальное
пространство,
социальные сети,
кеш файлы.

В статье анализируются виды следов при вымогательствах, совершаемых в сети Интернет, вопросы их выявления и получения.

Kompyuter texnologiyalari, shuningdek, Internetning rivojlanishi jinoyatlarning yangi turlarining, jumladan, Internet orqali sodir etilishiga imkoniyat yaratmoqda. Kompyuter xavfsizligi sohasidagi mutaxassislarining fikricha, kompyuter jinoyatlarining zarari g'iyohvand moddalar savdosi va turli o'g'irlik turlaridan keyin ikkinchi o'rinda turadi. Qolaversa, bu sohada jinoyatchilik yil sayin jadal sur'atlar bilan oshib bormoqda. Zamonaviy jamiyatda tashkilot va muassasalarning ko'pchiligi Internetda ishlaydigan turli xil texnik vositalardan foydalanadilar, masalan, elektron hujjat aylanishi, soliq va yuqori organlarga hisobot berish, elektron to'lovlar, hisob-kitoblar, turli ma'lumotlar bazalari va boshqalar. Internetdagi tovlamachilar olingan ma'lumotlardan o'z ixtiyoriga ko'ra foydalanadilar: ular uni foydali tarzda qayta sotadilar yoki tovlamachilik maqsadida foydalanadilar.

Ijtimoiy tarmoqlardagi tovlamachilik holatlari xalqaro jinoiy adliya idoralariga tobora ko'proq xabar qilinmoqda [1]. Shunga qaramay, rasmiy ma'lumotlarga ko'ra, ariza bilan murojaat qilishning kamligi sababli uning haqiqiy holatini baholash qiyin [2]. Tovlamachilikni o'rganish bo'yicha katta ish olib borilayotgan bo'lsa-da, ijtimoiy tarmoqlarda uning paydo bo'lishi haqida ma'lumotlar juda kam.

Ijtimoiy tarmoqlardagi tovlamachilik asta-sekin keng tarqalgan bo'lib, ma'lumotlar odatda ijtimoiy media profillaridan to'planadi yoki foydalanuvchilarning o'zidan aldab olinadi [3]. Kopecky chex yoshlarining 6-8 foizi (8-17 yoshdagi) ijtimoiy tarmoqlarda shantajga duchor bo'lganini aniqlagan [4]. Al Qahtani va uning hamkasblari 2018 yilda Saudiya Arabistonidagi kattalar orasida ijtimoiy tarmoqlarda shantaj ko'payganiga guvoh bo'lishgan, shantajchilar qurbonlardan naqd pul, jinsiy aloqa va boshqa ko'plab narsalarni talab qilishgan. Ummonda ijtimoiy tarmoqlarda shantaj holatlari ham ko'paygan, ba'zi qurbonlar tovlamachilik natijasida o'z joniga qasd qilishgan [5]. Yoki shunga o'xshab Fors ko'rfazi hamkorlik kengashi (GCC) mamlakatlarida ijtimoiy tarmoqlarda shantaj ko'payganligi haqida xabar berishgan, bunda yiliga 30 000 ta bunday hodisalar va ayollar bilan bog'liq bu hodisalarning 80 foizi shahvoniy kontent bilan bog'liq. Ijtimoiy tarmoqlarda bolalarni shantaj qilish, bu yerda erotik dalillar yoki rasmlar keyingi erotik materiallar, shahvoniy manfaatlar yoki naqd pul olishga majburlash uchun ishlatiladi [6]. Bundan tashqari, kompaniyalar ijtimoiy tarmoqlarda shantajga duchor bo'lishi mumkin, chunki shaxslar o'z obro'siga putur yetkazish bilan tahdid qilishadi [7].

Ushbu paragrafda biz Internet tarmog'i orqali sodir etilgan tovlamachilik jinoyati bo'yicha izlarni aniqlashning o'ziga xos xususiyatlarini: izlarning paydo bo'lish mexanizmi,

ularning manbalari hamda ularni aniqlash masalalarini ko'rib chiqamiz. Ushbu turdagi jinoyatlarda izlarni tezda sintez qilish eng yaxshi usuldir. Bu tegishli dalillarni o'z vaqtida va tejamkor tarzda taqdim etadi, ayniqsa tadqiqotning yangi va rivojlanayotgan sohalarida foydali bo'ladi hamda tizimli ko'rib chiqishdan unchalik farq qilmaydigan xulosalar beradi [8]. Bu jarayon qidiruv strategiyasini ishlab chiqish, qidiruv uchun tegishli ma'lumotlar bazalarini aniqlash, natijalarni kelishilgan mezonlar bo'yicha skrining qilish, natijalar sifatini baholash, ma'lumotlardan asosiy topilmalarni olish va paydo bo'ladigan asosiy mavzularning sintezini ta'minlashni o'z ichiga oladi [9].

Internetda tovlamachilikni tergov qilishda ushbu shaxslar to'g'risidagi ma'lumotlarni "Vkontakte", "Facebook", "Twitter", "Odnoklassniki", "My World" ijtimoiy tarmoqlarida, "Instagram", "YouTube" videoxosting saytlari va boshqalardan izlash maqsadga muvofiq.

Iz hosil qilish mexanizmi - bu iz hosil qilish jarayonining tarkibiy qismlari tizimi, iz hosil qiluvchi ob'ekt va uning iz moddasiga ta'sir qilish jarayoni [10].

Tovlamachilikning tabiati, uni amalga oshirish usuli va boshqa holatlar turli xil izlarning paydo bo'lishini belgilaydi.

Axborot texnologiyalari va Internetning zamonaviy rivojlanishi jinoyatchilarning fan va texnikaning ushbu yutuqlaridan foydalanib, turli jinoiy harakatlar, jumladan, tovlamachilikni sodir eta boshlashiga olib keldi.

Virtual makonning o'ziga xosligi shunda namoyon bo'ladiki, unda o'zaro ta'sir qiluvchi ob'ektlar (dastur va ma'lumotlar fayllari) va iz hosil qilishda (akslash jarayoni) ishtirok etadi.

Uyali aloqa va internet resurslaridan foydalangan holda sodir etilgan jinoyat izlarni shakllantirish mexanizmining o'ziga xos xususiyatlarini o'rganish "virtual izlar" tushunchasining paydo bo'lishiga olib keldi.

Virtual izlar – yaratish, kiritish, o'chirish, o'zgartirish, faollashtirish, ochish natijasida texnik qurilmalar, ularning tarmoqlari va tizimlari tomonidan axborot makonida qoldirilgan izlar [11].

Uyali aloqa va Internet resurslaridan foydalangan holda amalga oshirilgan zamonaviy tovlamachilik IP-manzillar, kesh-fayllar, jurnal fayllari, tarix jurnallari va boshqalar ko'rinishida virtual izlarni qoldiradi.

Tovlamachilik izining eng muhim elementi Internetda qoldirilgan ma'lumotlar, shu jumladan jabrlanuvchi bilan aloqalari (fotosuratlar, yozishmalar, videolar, elektron xabarlar va boshqalar) bilan bog'liq.

Mobil uyali aloqadan foydalangan holda tovlamachilikning odatiy izlari:

- aloqa operatorining elektron tashuvchisida: sessiya sanalari va ulanish davomiyligi haqida; provayderning dinamik yoki statik IP-manzil jurnallaridan ma'lumotlar va tegishli telefon raqamlari;

- mobil uyali aloqa qurilmasida - telefon abonent kitobi, uyali tarmoq abonentlarining ulanishlari to'g'risidagi ma'lumotlar (qo'ng'iroqlar jurnali, SMS, MMS), uyali aloqa tizimi, moliyaviy operatsiyalar, Skype, Facebook, Vkontakte va boshqalar ilovalari ma'lumotlari, iloji bo'lsa, mobil uyali aloqa foydalanuvchilarining ma'lumotlari, IMEI kodi, video va fotosuratlar, telefon raqamlari;

Virtual izlarni shakllantirish mexanizmlarini quyidagicha guruhlash mumkin:

1) Internetda paydo bo'ladigan iz hosil qiluvchi ob'ektlar (ma'lumotlar to'plami, tovush, tasvirlar, ish vaqti va boshqalar);

2) barcha turdagi serverlar (pochta serveri, katalog serveri, dastur serveri va boshqalar) resurslarida saqlanadigan ma'lumotlarning nusxasi.

Yuqoridagilarni umumlashtirib, biz quyidagi xulosalar chiqarishimiz mumkin:

1. Uyali aloqa va internet resurslaridan foydalangan holda tovlamachilikni sodir etishda iz hosil qilish mexanizmi an'anaviy (moddiy va ideal) va virtual izlarni o'z ichiga oladi.

2. Tovlamachilikning moddiy izlariga jabrlanuvchi tomonidan olingan anonim xatlar kiradi; qon dog'lari, jabrlanuvchining tanasidagi jarohatlar, qo'l, oyoq izlari, jinoyatchilar tomonidan qoldirilgan transport vositalari, jinoyatchi ushlab tashlab ketgan tovlamachilik buyumlari va boshqalar.

Tovlamachilikning ideal izlari, xususan, jabrlanuvchining xotirasida saqlanib qolgan jinoyatchining qiyofasi, uning gapirish uslubi, individual so'zlardan foydalanish va boshqalar.

3. Uyali aloqa va internet resurslaridan foydalangan holda sodir etilgan tovlamachilik IP-manzillar, kesh-fayllar, log-fayllar, tarix jurnallari va boshqalar ko'rinishidagi virtual izlarni qoldiradi.

Xalqaro miqyosdagi jinoyat statistikasida Internet tovlamachiligining tobora ko'payib borayotganiga qaramay, ijtimoiy tarmoqlarda shantajning paydo bo'lishi bo'yicha juda kam tadqiqot o'tkazilgan. Ushbu tadqiqotlarning yetishmasligi albatta salbiy oqibat bo'lib, u dalillarga asoslangan siyosatlar, amaliyotlar va aralashuvlarni ishlab chiqishga, shuningdek, bizning ushbu xatti-harakatni nazariy va tergov nuqtai nazaridan tushunishimizga to'sqinlik qilishi mumkin. Masalan, jinoyatchilar va uyushgan jinoiy guruhlar o'zlarini jabrlanuvchilar bilan onlayn aloqada bo'lib ko'rsatib, keyin ularni shantaj qilish orqali jabrdiyda qilishda rol o'ynashi mumkin bo'lsa-da, biz amaliyotda faqat jinoyatchilar va uyushgan jinoiy guruhlariga e'tibor qaratish, oflayn munosabatlarning sobiq hamkorlari qanday foydalanishi mumkinligi haqida bosh qotiramiz. Shuning uchun bizning bilimimizdagi bu bo'shliqni ushbu sohada samarali aralashuvlar, siyosat va amaliyotlarni ishlab chiqish haqida ma'lumot berish, masalan, ushbu faoliyatning yosh qurbonlari qanday va qachon xavf ostida bo'lishi mumkinligini tushunishimiz kerak. Boshqalarni shantaj qilish sodir bo'lishining va boshqalarning qurbon bo'lishiga yo'l qo'ymaslik uchun zarur bo'lgan mutaxassis yordamini olishini ta'minlashimiz mumkin.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ:

1. Al Qahtani, E., M. Shehab, and A. Aljohani. 2018. The effectiveness of fear appeals in increasing smartphone locking behavior among Saudi Arabians. <https://www.usenix.org/conference/soups2018/presentation/qahtani>.

2. Ahmed, A., E. Awad, S. Farouq, R. Ayesh, M. Mohammed, N. Alneqabi, M. Abdulahamid, and J. Ismail. 2017 Online blackmail. Crimes feed on the boom of social networking.

3. Monaghan, A. 2017. The impact of Self-Generated Images in online pornography. Middlesex University: Doctoral Dissertation. National Crime Council. 2020. Sextortion. <https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/kidnap-and-extortion/sextortion-webcam-blackmail>

4. Kopecky, K. 2017. Online blackmail of Czech children focused on so-called "sextortion" (analysis of culprit and victim Behaviours). Telematics and Informatics 34(1): 11-19.

5. Al Salehi, B. 2016. Blackmailing reportage for year 2016, Information Technology Authority. Oman.
https://ita.gov.om/ITAPortal/MediaCenter/Document_detail.aspx?NID=109.
6. EUROPOL. 2017. Online sexual coercion and extortion as a form of crime affecting children: law enforcement perspective. <https://www.europol.europa.eu/publications-documents/online-sexual-coercion-and-extortion-form-of-crime-affecting-children-law-enforcement-perspective>.
7. Raas, K.M.R. 2015. The threat of social media blackmailing in the hospitality industry: when customers misuse their power. Bachelor's thesis: University of Twente.
8. Khangura, S., K. Konnyu, R. Cushman, J. Grimshaw, and D. Moher. 2012. Evidence summaries: the evolution of a rapid review approach. *Systematic reviews* 1(1): 10.
9. Campbell, A., T. Forbes, A. McLaughlin, G. Davidson, M. Butler, C. Blair, N. Menabney and C. McKeaveney. 2019 Rapid evidence review: The relationship between alcohol and mental health problems. London: Alcohol Change UK.
10. Мещеряков В.А. Следы преступлений в сфере высоких технологий // Библиотека криминалиста: научный журнал. - 2013. - № 5 (10). - С. 267.
11. Савельева А.А., Савельева М.В. Значение «виртуальных» следов в криминалистике. - URL: http://www.rusnauka.com/18_NPRT_2017/Pravo/11_227043.doc.htm