BOJ PROTI DEZINFORMÁCIÁM: KĽÚČOVÁ ROLA DIGITÁLNYCH STÔP PRI ROZPOZNÁVANÍ HYBRIDNÝCH HROZIEB

FIGHTING DISINFORMATION: THE KEY ROLE OF DIGITAL TRACES IN IDENTIFYING HYBRID THREATS

JUDr. Branislav BELICA
Akadémia Policajného zboru v Bratislave
Sklabinská 1, 835 17 Bratislava, Slovenská republika
branislav.belica@akademiapz.sk

Abstrakt: Tento článok analyzuje kritickú úlohu digitálnych stôp v procese identifikácie a boja proti rozsiahlym dezinformačným kampaniam. V kontexte rastúceho nebezpečenstva v podobe hybridných hrozieb, ktoré cielene zneužívajú online priestor na manipuláciu a destabilizáciu spoločnosti, slúžia digitálne stopy ako esenciálny forenzný nástroj. Autor preto s využitím relevantných vedeckých metód skúma, ako sa pomocou digitálnej forenznej analýzy odhaľujú pôvodcovia, mechanizmy šírenia a prepojené siete aktérov stojacich za dezinformáciami. Poukazuje na to, že rozsiahle šírenie falošného obsahu sociálnymi médiami prehlbuje polarizáciu v spoločnosti a podkopáva dôveru v inštitúcie. Pre efektívnu a účinnú obranu je z uvedených dôvodov nevyhnutná kombinácia pokročilých metód detekcie, fact-checkingu a umelej inteligencie. Autor zároveň zdôrazňuje potrebu medziodborovej spolupráce medzi odborníkmi na kybernetickú bezpečnosť, tvorcami politík a profesionálmi z oblasti médií s cieľom zvýšiť odolnosť informačného priestoru voči manipulatívnym naratívom.

Kľúčové slová: Bezpečnosť, dezinformácie, digitálne stopy, hybridné hrozby,

Abstract: This article analyses the critical role of digital traces in the process of identifying and combating large-scale disinformation campaigns. In the context of the growing danger posed by hybrid threats, which deliberately exploit the online space to manipulate and destabilize society, digital traces serve as an essential forensic tool. Using relevant scientific methods, the author examines how digital forensic analysis helps uncover the originators, dissemination mechanisms, and interconnected networks of actors behind disinformation. He points out that the extensive spread of false content through social media deepens societal polarization and undermines trust in institutions. For effective and efficient defence, a combination of advanced detection methods, fact-checking, and artificial intelligence is therefore indispensable. The author also emphasizes the need for interdisciplinary cooperation among cybersecurity experts, policymakers, and media professionals in order to strengthen the resilience of the information space against manipulative narratives.

Keywords: Security, disinformation, digital traces, hybrid threats.

ÚVOD

V digitálne prepojenom svete sa šírenie informácií stalo mimoriadne rýchlym a intenzívnym. Moderné technológie a najmä široké možnosti online komunikácie umožnili masívne zdieľanie a šírenie rôzneho obsahu, no zároveň vytvorili priestor na zneužívanie týchto

nástrojov. V posledných rokoch dochádza k výraznému nárastu šírenia falošných správ, hoaxov, dezinformácií a propagandy, ktoré významne ovplyvňujú spoločnosť. Hlavným nástrojom ich distribúcie sa stali sociálne siete a internet, ktoré umožňujú anonymné a rýchle šírenie dezinformácií s minimálnymi nákladmi a bez priamej zodpovednosti.[1]

Sociálna a politická polarizácia v kombinácii s anonymitou online prostredia vytvára podmienky, v ktorých je možné efektívne manipulovať verejnou mienkou. Dezinformačné kampane narúšajú dôveru v štátne inštitúcie, destabilizujú demokratické procesy a využívajú práva, ako je sloboda prejavu, na podkopávanie samotného systému, ktorý ich garantuje. Ich dôsledky môžu byť rôznorodé – od ovplyvnenia volieb cez ekonomické škody až po ohrozenie verejného zdravia a bezpečnosti. Slovenská republika, rovnako ako iné krajiny, čelí týmto výzvam a hľadá spôsoby, ako efektívne bojovať proti škodlivým vplyvom dezinformácií.[2]

Kľúčovým krokom v boji proti dezinformáciám je analýza subjektov, ktoré ich šíria, a pochopenie ich motivácie. Keďže šíritelia dezinformácií môžu byť rôznorodí – od jednotlivcov až po organizované skupiny s politickými alebo ekonomickými cieľmi – neexistuje univerzálna stratégia na ich elimináciu. Aj preto je dôležité vytvoriť mechanizmy na identifikáciu a monitorovanie dezinformačných kampaní.[3]

Jednou z perspektívnych metód v tejto oblasti je využitie analýzy digitálnych stôp, ktoré zanechávajú užívatelia internetu pri svojej online aktivite. Digitálne stopy môžu poskytnúť dôležité informácie o pôvode dezinformácií, ich distribučných kanáloch a spôsobe, akým sa šíria medzi populáciou. Tradičné metódy overovania faktov často nestíhajú reagovať na rýchlosť šírenia dezinformácií, a preto rastie potreba využívania technológií, ako je umelá inteligencia a strojové učenie, na analýzu veľkých objemov dát. Tieto metódy môžu pomôcť identifikovať vzory správania, lokalizovať zdroje nepravdivých informácií a efektívnejšie zasahovať proti ich šíreniu.

Digitálne stopy umožňujú odhaliť pôvodcov falošných informácií, identifikovať ich šíriteľov a monitorovať rozsah ich dopadu. Ich skúmanie je nevyhnutné pre efektívnu obranu proti dezinformačným hrozbám a tvorbu účinných protiopatrení. Do budúcnosti sa očakáva, že analýza digitálnych stôp bude hrať čoraz dôležitejšiu úlohu pri zabezpečovaní informačnej integrity a ochrane spoločnosti pred negatívnymi dôsledkami dezinformácií.

1 DEZINFORMÁCIE AKO SÚČASŤ HYBRIDNÝCH HROZIEB

Dezinformácie predstavujú kľúčovú súčasť hybridných hrozieb a zahŕňajú úmyselné šírenie nepravdivých alebo zavádzajúcich informácií s cieľom manipulovať verejnosť. Ich

[1] IVANČÍK, R. 2024. Dezinformácie ako bezpečnostná hrozba šírená na internete. In *Auspicia*, 2024, roč. 21, č. 1, s. 26-36; BELICA, B. 2024. Subjekty regulujúce šírenie dezinformácií v podmien-kach Slovenskej republiky a mimio nej. In *Trilobit*, 2024, roč. 16, č. 1, 1-22; SABAYOVÁ, M. 2024. Sebavnímanie odolnosti voči dezinformáciám vo vysokoškolskom prostredí. In *Auspicia*, 2024, roč. 21, č. 1, s. 59-71.

[2] HAJDÚKOVÁ, T. 2024. Zdroje informácií alebo dezinformácií. In *Auspicia*, 2024, roč. 21, č. 1, s. 37-49. ISSN 2464-7217; DUŠEK, J. – KAVAN, Š. 2023. Dezinformace jako součást hybridních hrozeb pohledem studentů VŠERS. In *Interpolis*, 2023, s. 7-25; ZACHAR KUCHTOVÁ, J. 2022. Bezpečnosť na sociálnych sieťach. In *Bezpečnosť elektronickej komunikácie : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2022, s. 237-247.

[3] IVANČÍK, R. 2025. *Dezinformácie. Teoretické východiská ich skúmania*. Praha: Leges, 2025; DUŠEK, J. – KAVAN, Š. 2024. Dezinformace jako součást hybridních hrozeb – česko-slovenský pohled. In *Auspicia*, 2024, roč. 21, č. 1, s. 7-25; NOVÁKOVÁ, I. 2022. Boj proti dezinformáciám z pohľadu študentov In *Dezinformácie a právo (úlohy a postavenie bezpečnostných zložiek) : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2020, s. 176-188

účelom môže byť politická a ekonomická destabilizácia, ovplyvňovanie volieb, vyvolanie paniky alebo zníženie dôvery vo verejné inštitúcie.

Dezinformácie sa môžu šíriť rôznymi spôsobmi, napríklad :

- Manipuláciou faktov – skreslenie alebo vytrhnutie informácií z kontextu s cieľom vyvolať nesprávne interpretácie.
- Deepfake technológiami – vytváranie falošných videí alebo zvukových nahrávok s cieľom diskreditovať osoby alebo inštitúcie.
- Sociálnymi botmi a trollmi – automatizované alebo platené účty na sociálnych sieťach, ktoré šíria propagandu a ovplyvňujú diskusie.[4]

Hybridné hrozby a dezinformácie sú úzko prepojené fenomény, pričom dezinformácie predstavujú jeden z hlavných nástrojov hybridnej vojny. Pojmy hybridná hrozba a hybridná vojna sa od anexie Krymu čoraz častejšie objavujú v bezpečnostných diskusiách. Predstavujú aktivity realizované štátnymi alebo neštátnymi aktérmi s cieľom ovplyvniť rozhodovacie procesy cieľovej krajiny na úrovni štátu, inštitúcií alebo regiónov a tým jej spôsobiť škodu. Nástroje hybridných operácií umožňujú dosahovanie strategických cieľov aj bez formálneho vyhlásenia vojny. Existuje mnoho spôsobov, ako takéto aktivity vykonávať, pričom jednou z efektívnych metód sú dezinformačné kampane. Tie slúžia nielen na ovplyvňovanie verejnej mienky, ale aj na radikalizáciu, nábor alebo manipuláciu podporovateľov určitých ideológií.[5]

V kontexte dezinformácií ako hybridnej hrozby je dôležité zdôrazniť, že ich šírenie patrí medzi základné nástroje informačnej vojny. Tá zahŕňa široké spektrum operácií, ktoré možno rozdeliť do viacerých kategórií, ako sú kybernetické útoky, psychologické operácie, spravodajské aktivity, diskreditačné kampane či systematické zavádzanie verejnosti. Strategické využívanie dezinformácií a propagandy zo strany nepriateľského aktéra tak môže byť považované za neoddeliteľnú súčasť informačnej vojny, ktorej cieľom je oslabenie politickej stability, narušenie dôvery v inštitúcie či rozdelenie spoločnosti.[6]

Dezinformácie môžu byť taktiež priamo prepojené s kybernetickými útokmi. Napríklad, falošné správy môžu obsahovať odkazy na škodlivé webové stránky alebo vyzývať používateľov na stiahnutie súborov, ktoré v skutočnosti obsahujú malvér. Takéto metódy demonštrujú, že šírenie dezinformácií môže byť integrovaným nástrojom hybridných operácií, kde sa kombinujú psychologické a technické aspekty s cieľom manipulovať, destabilizovať a poškodiť cieľové subjekty.

Praktické príklady využitia dezinformácií v rámci hybridných hrozieb zahŕňajú:

- Ovplyvňovanie volieb – cieľom môže byť zmena verejnej mienky prostredníctvom falošných naratívov o kandidátoch alebo politických stranách.

---

[4] MARWICK, A. – LEWIS, R. 2017. Media Manipulation and Disinformation Online [online]; ZACHAR KUCHTOVÁ, J. 2024. Šírenie dezinformácií s využitím nástrojov umelej inteligencie. In Dušek, J. a kol.: *Dezinformace ve střední Evropě: vývoj, právní rámce a bezpečnostní dopady v éře umělé inteligence a digitálních technologií*. České Budějovice : Vysoká škola evropských a regionálních studií, 2024. s. 90-107

[5] IVANČÍK, R. – NEČAS, P. 2025. *Hybridné hrozby: Bezpečnostná výzva pre demokratické spoločnosti*. Praha: Leges, 2025; DUŠEK, J. – KAVAN, Š. 2024. Dezinformace jako součást hybridních hrozeb – česko-slovenský pohled. In *Auspicia*, 2024, roč. 21, č. 1, s. 7-25; IVANČÍK, R. 2023. On Disinformation and Propaganda in the Context of the Spread of Hybrid Threats. In Vojenské reflexie, 2023, roč. 18, č. 3, s. 38-58

[6] VEJVODOVÁ, P. 2019. Information and Psychological Operations as a Challenge to Security and Defence. In. *Vojenské rozhledy* [online]. č.3/2019. s. 85-86; BURZALA, D. 2024. Dezinformácie ako „nová hrozba“ pre spoločnosť. In *Bezpečnosť elektronickej komunikácie : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2024, s. 50-63

- Šírenie paniky a nedôvery – manipulácia správ o zdravotných hrozbách, ekonomických krízach alebo vojenských konfliktoch s cieľom destabilizácie štátu.
- Oslabenie medzinárodných aliancií – snahy o narušenie dôvery medzi spojencami prostredníctvom falošných obvinení a konšpiračných teórií.

Keďže dezinformácie sú jedným z najúčinnejších nástrojov hybridných hrozieb, je nevyhnutné zamerať sa na ich detekciu a elimináciu. Efektívny boj proti dezinformáciám zahŕňa kombináciu technologických riešení, mediálnej gramotnosti a legislatívnych opatrení. V tomto smere môže hrať dôležitú úlohu aj analýza digitálnych stôp, ktorá umožňuje sledovať pôvod a šírenie manipulatívneho obsahu.[7]

2 ROZPOZNÁVANIE DEZINFORMÁCIÍ V ONLINE PRIESTORE

Na účinné rozpoznanie dezinformácií je potrebné poznať ich charakteristické znaky. Po ich úspešnom identifikovaní je možné prejsť k vyhľadávaniu, zaisťovaniu a skúmaniu digitálnych stôp. Európsky parlament v kontexte uvedeného vypracoval príručku s názvom „Ako odhaliť falošnú správu“ s cieľom efektívne bojovať proti dezinformáciám. Podľa tejto príručky približne 85 % Európanov vníma „falošné správy“ ako problém vo svojej krajine, pričom 83 % ich považuje za hrozbu pre demokraciu ako celok.

Príručka uvádza osem krokov, ktoré môžu pomôcť pri identifikácii falošných správ. Táto príručka je vypracovaná odborníkmi z praxe, pričom uvádza cenné informácie, ktoré môžu byť implementované pri identifikácií dezinformácií či už odborníkmi alebo laickou verejnosťou.

Úvodným krokom je overenie obsahu, pri ktorom je dôležité sústrediť sa na presnosť faktov, prípadnú zaujatosť a jednostrannosť článku. Dôveryhodné médiá, ktoré sa riadia etickým kódexom, zabezpečujú vyvážené informovanie a poskytujú priestor na vyjadrenie rôznych názorov, pričom subjektívne stanoviská bývajú vyhradené pre blogy a komentáre. Overovaniu faktov sa profesionálne venujú takzvaní *fact-checkeri*, pričom vo väčšine prípadov ide o novinárov, alebo členov rôznych mimovládnych organizácií.

Druhým krokom je preverenie samotného zdroja informácie. Kľúčovým aspektom je rozpoznanie, či ide o známe médium. Väčšina renomovaných médií na Slovensku aj vo svete je verejne známa, avšak na internete sa objavujú platformy s nejasným pôvodom, vlastníctvom či financovaním. Takéto médiá predstavujú potenciálne riziko, najmä ak ich domény sú registrované v zahraničí a nie je možné dohľadať ich skutočných prevádzkovateľov. Vysokú mieru opatrnosti si vyžadujú práve tie médiá, ktorých transparentnosť a objektivita sú spochybniteľné. Aj preto sa analytici pri identifikácií dezinformácií zameriavaju najmä na neznáme zdroje.

Ďalším dôležitým krokom pri overovaní dôveryhodnosti informácií je preverenie autora a zdroja príspevku. Mnohé dezinformačné weby nezverejňujú mená autorov a namiesto toho sa odvolávajú na zahraničné zdroje, neznáme či dokonca fiktívne osoby a organizácie. Na druhej strane môže byť autor síce známy, avšak spojený s dezinformačným prostredím, kde systematicky šíri manipulatívny obsah. Často ide o takzvaných komerčných dezinformátorov,

[7] BELICA, B. 2024. Vybrané legislatívne možnosti regulácie šírenia dezinformácií. In *Bezpečnosť elektronickej komunikácie : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2024, s. 10-21; HAŠANOVÁ, J. 2024. Administratívno-právne aspekty boja proti dezinformáciám. In Dušek, J. a kol.: *Dezinformace ve střední Evropě: vývoj, právní rámce a bezpečnostní dopady v éře umělé inteligence a digitálních technologií*. České Budějovice : Vysoká škola evropských a regionálních studií, 2024. s. 141-164

ktorých cieľom je šíriť zavádzajúce informácie pre osobný prospech. Bežnou praktikou je tiež zneužitie mena známej osobnosti, ktorá v skutočnosti s prezentovaným obsahom nemá nič spoločné, ale jej autorita má zvýšiť dôveryhodnosť klamlivého materiálu.

Dôležitou súčasťou procesu overovania je aj analýza obrázkov a videí, ktoré môžu byť zmanipulované alebo vytrhnuté z kontextu. Na tento účel možno využiť nástroje ako Google Lens, ktorý umožňuje vyhľadať zdroj obrázka, alebo modul InVID, ktorý pomáha odhaliť úpravy a manipulácie s multimediálnym obsahom. Častým príkladom je použitie fotografií z databáz či starších udalostí, ktoré sú prezentované ako aktuálne a spojené s inými udalosťami. Napríklad zábery masových protestov môžu byť nesprávne označené ako demonštrácie v inej krajine či v inom časovom kontexte, čím sa vytvára falošný dojem o situácii.

Pri odhaľovaní dezinformácií je kritické zváženie obsahu ďalším dôležitým krokom. Väčšina hoaxov a manipulatívnych správ je koncipovaná tak, aby emocionálne zasiahla čitateľa a motivovala ho k ich ďalšiemu šíreniu. Často sa používajú senzačné titulky, ktoré vyvolávajú strach, pobúrenie alebo silné emócie. Typickou taktikou dezinformátorov je vytváranie ilúzie naliehavosti, napríklad prostredníctvom výrokov ako „pravda konečne vyšla najavo, zdieľajte, kým to nezmažú“. Ľudia, ktorí takéto príspevky šíria, môžu nadobudnúť pocit výnimočnosti, že „odhalili skrytú pravdu“, čím sa stávajú nevedomými súčasťami šírenia manipulácie.

Jedným z kľúčových varovných signálov je príliš dramatický alebo senzačný príbeh, ktorý sa zdá byť až príliš výnimočný na to, aby bol pravdivý. Spoľahlivým spôsobom jeho overenia je kontrola, či sa danej téme venujú aj renomované médiá. Ak ide o skutočne významnú udalosť, bude pokrytá aj dôveryhodnými zdrojmi, ktoré sa riadia etickými štandardmi žurnalistiky. Dezinformátori však často cielene podkopávajú dôveru v etablované médiá a vytvárajú naratív, že iba oni prinášajú „skutočné“ informácie. Takýmto spôsobom si budujú základňu verných podporovateľov, ktorí ich nielen pravidelne sledujú, ale aj finančne podporujú.

Mnohé dezinformačné platformy okrem skrytého financovania získavajú príspevky od bežných čitateľov, pričom sa prezentujú ako nezávislé médiá financované výhradne svojimi odberateľmi. Táto forma sebaprezentácie má zvýšiť ich domnelú dôveryhodnosť a zároveň minimalizovať náklady na prevádzku. Niektoré weby dokonca zverejňujú údaje o vyzbieraných finančných príspevkoch, pričom výška uvedenej sumy môže byť nepravdivá. Časť financií môže pochádzať priamo od osôb alebo organizácií, ktoré dané médiá v skutočnosti riadia, čím vytvárajú falošný dojem masívnej verejnej podpory.

Posledným krokom k efektívnemu odhaľovaniu dezinformácií je neustále vzdelávanie v oblasti mediálnej gramotnosti a kritického myslenia. Sledovanie relevantných webov a organizácií, ktoré sa venujú boju proti dezinformáciám, pomáha identifikovať manipulatívne techniky a zvyšovať schopnosť rozlišovať medzi dôveryhodnými a zavádzajúcimi informáciami. V súčasnom digitálnom prostredí je dôležité neustále rozvíjať schopnosť kritického hodnotenia obsahu a nepodliehať emocionálne nabitým a jednostranným tvrdeniam bez ich riadneho overenia.[8]

Odporúčania na identifikáciu dezinformácií poskytuje aj Európske stredisko pre monitorovanie digitálnych médií (European Digital Media Observatory – EDMO). Táto iniciatíva, financovaná Európskou úniou, funguje ako nezávislá platforma združujúca overovateľov faktov, výskumníkov a ďalšie subjekty zapojené do boja proti dezinformáciám. V rámci svojho výskumu odborníci z EDMO definovali päť základných krokov, ktoré pomáhajú odhaliť dezinformácie a posilniť individuálnu odolnosť voči zavádzajúcim informáciám.

[8] BENTZEN, N. 2019. *Ako odhaliť falošnú správu*. [online]

Prvým a najdôležitejším krokom je kritické myslenie a kontrola vlastných emócií. Dezinformácie sú často formulované tak, aby vyvolávali silnú emocionálnu reakciu, ktorá môže oslabiť racionálne uvažovanieImpulzívne reakcie sú totiž hlavným faktorom, ktorý prispieva k nekontrolovateľnému šíreniu hoaxov na internete.

Ďalším dôležitým krokom je overenie, či rovnakú informáciu priniesli aj iné zdroje. Táto zásada je spoločná s odporúčaniami Európskeho parlamentu, čo len potvrdzuje jej význam. Dôveryhodné správy sú zvyčajne pokryté viacerými relevantnými médiami, zatiaľ čo dezinformácie často pochádzajú z pochybných alebo anonymných zdrojov.

Tretím krokom je využitie pokročilých vyhľadávacích nástrojov na overenie obrázkov a videí. Obrazový materiál býva často vytrhnutý z kontextu alebo zámerne upravený s cieľom zavádzať verejnosť. Na identifikáciu pôvodu obrázkov je možné použiť nástroje ako Google Lens alebo InVID, ktoré pomáhajú určiť, či bol vizuálny obsah zmanipulovaný alebo nesprávne interpretovaný.

Štvrtý krok zdôrazňuje ostražitosť voči senzáciám. Dezinformačné správy často využívajú senzačné titulky a nepravdepodobné tvrdenia, ktoré sa riadia jednoduchým pravidlom: ak niečo vyznieva príliš dobre alebo zle na to, aby to bola pravda, pravdepodobne pravda nie je. Senzácie a konšpiračné teórie sú navrhnuté tak, aby oslovili emócie ľudí a podnietili ich k nekritickému prijímaniu informácií.

Piatym a zároveň posledným odporúčaním EDMO, ktoré dopĺňa odporúčania Európskeho parlamentu, je využívanie fakt-checkingových platforiem na overovanie podozrivých tvrdení. Ak má človek pochybnosti o pravdivosti určitej informácie, je veľká pravdepodobnosť, že sa jej už venovali overovacie webové stránky. Medzi známe platformy na kontrolu faktov patria DW Fact Check, EUvsDisinfo, AFP Fact Check a mnohé ďalšie, ktoré poskytujú podrobné analýzy a vyvracajú zavádzajúce tvrdenia.

Tieto informácie vytvárajú základný teoretický rámec identifikácie dezinformácií, pričom sú zamerané aj na predchádzanie ich ďalšiemu šíreniu. Uvedené fakty je preto možné uplatniť nie len v rámci užívateľského prostredia, ale aj analytickej činnosti.[9]

3 POJEM DIGITÁLNA STOPA

Identifikácia dezinformácií predstavuje prvý a zásadný krok v boji proti šíreniu nepravdivých a manipulatívnych informácií. Samotné odhalenie nepravdivého obsahu však nepostačuje, ak chceme pochopiť jeho pôvod, mechanizmus šírenia a celkový dosah na spoločnosť. Práve v tomto kontexte nadobúda kľúčový význam analýza digitálnych stôp, ktoré dezinformácie zanechávajú v online priestore.

Z hľadiska kriminalistiky je digitálna stopa definovaná ako akákoľvek zmena v digitálnom prostredí, ktorá obsahuje informácie súvisiace s kriminalisticky významnou udalosťou. Táto stopa je dostupná, uchovávaná alebo prenášaná v digitálnej podobe a možno ju identifikovať pomocou kriminalistickej informatiky.[10]

Podľa Meteňka a Meteňkovej digitálna stopa vzniká, prenáša sa, ukladá a archivuje v digitálnej forme ako elektrický, magnetický, optický alebo iný podobný prejav poľa. Po jej uložení sa zhmotňuje na pamäťovom médiu, pričom jej záznam má charakter poľa. Aby bolo možné prenášané informácie analyzovať, je potrebné ich najskôr technologicky zachytiť a

[9] EURÓPSKA KOMISIA. 2022. *Ako nepodľahnúť dezinformáciám? Prinášame päť tipov od odborníkov*. [online]
[10] METEŇKO, J., METENKOVÁ, M., 2024. Digital trace as a personal and criminalistics object – In *Security Horizons*, Faculty of security, Skopje, 2024 , International scientific conference contemporary security challenges and strengthening the resilience of the countries of southeast europe, s. 175-191

následne dočasne alebo trvalo uložiť na pamäťové médium. Z fyzikálneho hľadiska má digitálna stopa zanedbateľnú hmotnosť, avšak materiálnu podstatu. To znamená, že sa na ňu aplikuje teória odrazu, teda sa charakteristiky odrazeného predmetu prenášajú na predmet odrážajúci. Digitálna stopa je teda stopou vnútornej štruktúry odrazeného objektu a vonkajšie znaky sa prejavujú vo formáte, v akom je aktuálne uložená.[11]

Digitálne stopy umožňujú skúmať, kto a akým spôsobom stojí za šírením falošných správ, aké komunikačné kanály využíva a aký je dosah týchto informácií na cieľovú populáciu. Prostredníctvom analýzy metadát, IP adries, registrácie domén či správania účtov na sociálnych sieťach možno identifikovať nielen jednotlivých aktérov, ale aj celé siete zapojené do koordinovaných dezinformačných operácií.

Skúmanie digitálnych stôp umožňuje rozlíšiť medzi náhodným šírením nepravdivých informácií nevedomými jednotlivcami a systematickou informačnou kampaňou riadenou konkrétnymi záujmovými skupinami. Taktiež poskytuje dôležité poznatky o tom, aké nástroje a stratégie dezinformátori využívajú na maximalizáciu dosahu svojho obsahu, vrátane algoritmov sociálnych sietí, botov či falošných účtov.

Prepojenie identifikácie dezinformácie s jej ďalšou analýzou cez digitálne stopy je nevyhnutné na odhalenie širšieho kontextu informačných operácií. Zatiaľ čo identifikácia umožňuje rozpoznať nepravdivý obsah, analýza digitálnych stôp ponúka možnosť sledovať jeho šírenie, určiť jeho pôvod a poskytnúť informácie, ktoré môžu ďalej slúžiť ako podklady pri navrhovaní efektívnych opatrení na obmedzenie jeho dopadu.

Digitálna stopa predstavuje súbor údajov, ktoré vznikajú v dôsledku aktivity používateľa v digitálnom prostredí. Každá interakcia s digitálnym zariadením, či už ide o prehliadanie webových stránok, komunikáciu na sociálnych sieťach, používanie aplikácií alebo odosielanie e-mailov, zanecháva jedinečné digitálne stopy, ktoré môžu byť použité na identifikáciu konkrétneho používateľa alebo zariadenia.[12]

Digitálna stopa je úzko prepojená s konceptom digitálnej identity a predstavuje súhrn všetkých informácií, ktoré je možné o osobe alebo organizácii získať na základe ich online aktivity. Okrem sledovania správania jednotlivcov a skupín sa digitálne stopy využívajú na analýzu a vyhodnocovanie nazbieraných dát, čo je dôležité v oblasti kybernetickej bezpečnosti, vyšetrovania trestných činov ale aj marketingu.

Digitálne stopy môžeme rozdeliť podľa spôsobu vzniku do dvoch hlavných kategórií:

- Aktívna digitálna stopa – vzniká, keď užívateľ vedome zanechá údaje na internete alebo iných digitálnych platformách, napríklad pri zverejňovaní príspevkov na sociálnych sieťach, odosielaní e-mailov alebo zadávaní údajov do online formulárov.
- Pasívna digitálna stopa – vzniká bez priameho vedomia užívateľa, často automaticky, napríklad prostredníctvom cookies, IP adries, časových záznamov prístupu na webové stránky či metadát ukladaných pri používaní smartfónov a aplikácií.[13]

Tieto stopy sú využívané na rôzne účely, od personalizácie reklám a analytiky správania užívateľov až po vyšetrovanie a sledovanie potenciálnych hrozieb v kyberpriestore.

---

[11] METEŇKO, J. a METEŇKOVÁ, M. 2024. Kriminalistický a personálny prístup ku skúmaniu digitálnej stopy. In Udržitelný rozvoj XV: 20 let členství v EU: Úspěchy, výzvy a perspektivy, České Budejovice : VŠERS, 2024

[12] ESET. 2021. *Vaša digitálna stopa: Čo to je a ako sa o ňu starať.* [online]

[13] ESET. 2021. *Čo je to digitálna stopa?* [online]

Podľa vedomia používateľa o jej vytvorení rozlišujeme digitálne stopy na:

- vedomú digitálnu stopu,
- nevedomú digitálnu stopu.

Vedomá digitálna stopa predstavuje informácie, ktoré používateľ cielene a úmyselne zanecháva pri svojej interakcii v digitálnom prostredí. Ide o údaje, ktoré sú výsledkom aktívnej činnosti jednotlivca na internete a digitálnych zariadeniach, pričom si je vedomý ich vytvorenia, ukladania a potenciálneho spracovania tretími stranami.

Typickými príkladmi vedomej digitálnej stopy sú:

- Publikovaný obsah na sociálnych sieťach – príspevky, komentáre, reakcie a zdieľania na platformách ako Facebook, Twitter, Instagram či LinkedIn.
- E-mailová komunikácia – správy odosielané prostredníctvom elektronickej pošty, ktoré obsahujú osobné údaje, pracovné informácie alebo citlivé súbory.
- Registrácia a vytváranie účtov – vytvorenie profilu na rôznych platformách, online nakupovanie, diskusné fóra či predplatné služieb.
- Účasť v online diskusiách a blogoch – publikovanie článkov, komentárov a iného obsahu, ktorý je spätý s konkrétnym používateľom.
- Digitálne podpisy a elektronické dokumenty – právne záväzné dokumenty alebo zmluvy, ktoré obsahujú jednoznačnú identifikáciu osoby.

Používateľ pri tvorbe vedomej digitálnej stopy často očakáva určitú formu spätnej väzby, interakcie či odozvy zo strany ostatných používateľov internetu. Avšak aj napriek tomu, že ide o úmyselne vytvorenú stopu, jej rozsah a následky nemusia byť plne predvídateľné. Informácie zverejnené na internete môžu byť šírené ďalej, ukladané na rôznych serveroch a analyzované tretími stranami, čím môže dôjsť k ich zneužitiu.

Nevedomá digitálna stopa pozostáva z údajov, ktoré používatelia zanechávajú pri využívaní digitálnych technológií bez toho, aby si tento proces uvedomovali. Ide o informácie generované automaticky prostredníctvom systémových procesov, algoritmov a analytických nástrojov, pričom ich zaznamenávanie často prebieha na pozadí bez priameho zásahu používateľa.

Medzi hlavné zdroje nevedomej digitálnej stopy patria:

- IP adresa a geolokácia – pri každom pripojení k internetu sa zaznamenáva IP adresa zariadenia, ktorá môže odhaliť približnú polohu používateľa a jeho poskytovateľa internetových služieb.
- Cookies a sledovacie technológie – webové stránky ukladajú súbory cookie do zariadení používateľov s cieľom uchovávať údaje o ich preferenciách, nákupoch či prezeranej histórii. Okrem toho môžu byť využité aj reklamnými sieťami na sledovanie online správania.
- História prehliadania a vyhľadávacie dotazy – internetové prehliadače zaznamenávajú, aké stránky používatelia navštívili a aké výrazy vyhľadávali, čo môže byť neskôr použité na personalizáciu reklám alebo analýzu spotrebiteľského správania.
- Metaúdaje – aj keď používateľ vedome komunikuje prostredníctvom e-mailov alebo mobilných aplikácií, systém automaticky generuje metaúdaje, ktoré obsahujú informácie o odosielateľovi, príjemcovi, čase a mieste komunikácie.
- Používanie aplikácií a zariadení – mobilné telefóny a inteligentné zariadenia zbierajú údaje o tom, ako ich používateľ využíva, vrátane počtu krokov, času stráveného v aplikáciách, hlasových príkazov a interakcií so systémom.

Nevedomá digitálna stopa predstavuje významné riziko z pohľadu ochrany súkromia, keďže používatelia si často neuvedomujú, aké údaje sú o nich zaznamenávané a kto k nim má prístup.[14]

V anglicky hovoriacich krajinách sa pojmy „digital footprint“ (digitálna stopa) a „digital evidence“ (digitálny dôkaz) často používajú zameniteľne, pričom dôraz je kladený na právnu a forenznú hodnotu údajov. Digitálne dôkazy sú podmnožinou digitálnych stôp, pričom ich využiteľnosť závisí od ich autenticity, integrity a schopnosti byť akceptované súdom.

Na rozdiel od bežnej digitálnej stopy, ktorá môže obsahovať aj údaje bežnej užívateľskej aktivity, digitálny dôkaz musí byť riadne zdokumentovaný, aby bol právne relevantný. V tomto kontexte je dôležité, aby boli digitálne dôkazy správne získavané, uchovávané a analyzované v súlade s príslušnou metodikou.

Digitálne stopy sa nachádzajú v rôznych technologických systémoch a ich zdroje môžeme rozdeliť do troch hlavných kategórií:

1. Otvorené počítačové systémy – osobné počítače, notebooky, servery, pevné disky, cloudové úložiská.
2. Komunikačné systémy – pevné a mobilné telefóny, e-mailové servery, počítačové siete, internetové protokoly, sociálne médiá.
3. Zariadenia s integrovanými čipmi – smartfóny, platobné karty, navigačné systémy GPS, palubné počítače automobilov, inteligentné domáce zariadenia.[15]

Tieto systémy generujú obrovské množstvo dát, ktoré môžu byť využité nielen na analýzu užívateľského správania, ale aj na odhaľovanie kybernetických hrozieb, monitorovanie podozrivých aktivít či optimalizáciu bezpečnostných opatrení.

Vzhľadom na exponenciálny nárast digitálnych údajov je potrebné neustále zlepšovať metódy ich analýzy a ochrany. Digitálne stopy poskytujú neoceniteľné informácie, no zároveň predstavujú výzvu v oblasti etiky, regulácie a ochrany osobných údajov.[16]

4 ZAISŤOVANIE DIGITÁLNYCH STÔP

Zaisťovanie digitálnych stôp predstavuje kľúčový proces pri vyšetrovaní trestnej činnosti, kde zohrávajú digitálne dôkazy dôležitú úlohu pri objasňovaní skutkového stavu a identifikácii páchateľov. Orgány činné v trestnom konaní musia pri práci s digitálnymi dôkazmi postupovať v súlade so zákonom, aby boli tieto dôkazy neskôr použiteľné v súdnom konaní.

V slovenskom právnom systéme je proces zaisťovania digitálnych dôkazov upravený v Trestnom poriadku (§90 a nasl. zákona č. 301/2005 Z. z.), ktorý stanovuje postupy pri domových prehliadkach, osobných prehliadkach, prehliadkach iných priestorov a pozemkov, odňatí a vydaní vecí, obhliadkach miesta činu či uchovaní, vydaní a odňatí počítačových údajov. Každý z týchto úkonov musí byť vykonaný v súlade s právnymi predpismi, aby bola zachovaná integrita dôkazového materiálu.

Proces zaisťovania digitálnych dôkazov začína v okamihu, keď sú údaje obsahujúce relevantné informácie alebo zariadenia, na ktorých sú takéto dáta uložené, zaistené na ďalšie

[14] INTERNETEM BEZPECNE. 2025. *Digitální stopa*. [online]
[15] METEŇKO, J., METENKOVÁ, M., 2024. Digital trace as a personal and criminalistics object – In *Security Horizons*, Faculty of security, Skopje, 2024, International scientific conference contemporary security challenges and strengthening the resilience of the countries of southeast europe, s. 175-191
[16] PORADA, V. a kol. 2019. Kriminalistika. Technické, forenzní a kybernetické aspekty. 2. vyd. Plzeň: Aleš Čeněk, 2019. s. 192-193

skúmanie. Zaisťovanie môže prebiehať viacerými spôsobmi v závislosti od charakteru prípadu a prostredia, v ktorom sa digitálne dôkazy nachádzajú.

Medzi základné úkony patrí fyzické zaistenie hardvéru, na ktorom môžu byť uložené relevantné digitálne dôkazy. Ide najmä o:

- osobné počítače, notebooky, servery,
- pevné disky, USB kľúče, pamäťové karty, CD a DVD médiá,
- mobilné telefóny, tablety, inteligentné zariadenia,
- sieťové prvky ako routery, firewally či dátové servery.

Pri zaistení týchto zariadení sa zabezpečuje, aby nedošlo k neoprávnenej manipulácii s dátami, čo zahŕňa používanie špeciálnych forenzných nástrojov na ochranu integrity digitálnych dôkazov. Kľúčovou metódou je vytváranie bitových kópií úložných médií, ktoré umožňujú ďalšiu analýzu bez poškodenia pôvodných dát.

Digitálne dáta môžu byť zaistené viacerými spôsobmi, pričom každý z nich musí zabezpečiť ich autenticitu a dôkaznú hodnotu:

- Kopírovanie dát – napríklad zo serverov, cloudu alebo databáz za prítomnosti správcu systému.
- Zachytenie sieťovej komunikácie – monitorovanie prenosu dát medzi zariadeniami alebo cez internet.
- Zaisťovanie e-mailovej komunikácie – analýza elektronickej pošty a jej metadát.
- Zaistenie dát zo sociálnych sietí a webových stránok – identifikácia online komunikácie a interakcií.
- Archivácia logovacích súborov – spracovanie dát z bezpečnostných protokolov systémov.

Tieto úkony sa vykonávajú s cieľom uchovať dôkazový materiál v pôvodnej forme, aby sa minimalizovalo riziko jeho poškodenia alebo zneužitia. Rovnako, ak to situácia dovoľuje, je dôležité mať k dispozícii originál digitálnej stopy, nakoľko pri vytváraní kópie môže byť zaistená iba určitá časť, čo môže sťažiť proces dokazovania v zmysle zásady „pochybosti v prospech obvineného“.[17]

Po zaistení digitálnych dôkazov nasleduje ich podrobná analýza, ktorá zahŕňa:

- Obnovu vymazaných súborov a dát – využitie špecializovaných softvérov na obnovenie zmazaných informácií.
- Analýzu metadát – skúmanie časových záznamov, IP adries a ďalších informácií o manipulácii so súbormi.
- Zisťovanie súvislostí medzi digitálnymi stopami – sledovanie reťazcov e-mailovej komunikácie, prístupu k systémom či interakcií na sociálnych sieťach.
- Použitie kryptografických metód na dešifrovanie údajov – analýza zašifrovaných diskov a súborov.

Forenzná analýza digitálnych dôkazov je nevyhnutná pre preukázanie ich pravosti a zabezpečenie ich použiteľnosti v trestnom konaní. Orgány činné v trestnom konaní spolupracujú so súdnymi znalcami v oblasti informačných technológií, ktorí vykonávajú podrobné skúmanie digitálnych stôp.[18]

---

[17] PORADA, V. a kol. 2019. Kriminalistika. Technické, forenzní a kybernetické aspekty. 2. vyd. Plzeň: Aleš Čeněk, 2019, s. 188

[18] METĚNKO, J. a kol. 2004. Kriminalistické metódy a možnosti kontroly sofistikovanej kriminality. Katedra kriminalistiky a forenzných disciplín, Akadémia PZ v Bratislave. Bratislava 2004. s. 356

Zaisťovanie digitálnych dôkazov prináša niekoľko výziev, medzi ktoré patrí:

- Technologická zložitosť – neustále sa vyvíjajúce technológie sťažujú schopnosť vyšetrovania zachytiť a analyzovať všetky relevantné dáta.
- Šifrovanie a anonymizácia – mnohé digitálne systémy používajú metódy ochrany údajov, ktoré sťažujú prístup k digitálnym dôkazom.
- Riziko zmeny alebo straty dát – nesprávna manipulácia s digitálnymi dôkazmi môže viesť k ich poškodeniu alebo strate dôkaznej hodnoty.
- Právne obmedzenia – zhromažďovanie digitálnych stôp musí byť vykonané v súlade s legislatívou, aby bolo možné tieto dôkazy použiť v súdnom konaní.

Digitálne stopy sa vyznačujú množstvom charakteristík, medzi ktoré patrí ich početnosť, latencia, časová sledovateľnosť a vysoký obsah informácií. Ich životnosť je veľmi nízka, pričom objem údajov môže byť značný. S rozvojom nových technológií dochádza k poklesu hustoty dát digitálnych stôp, zatiaľ čo prostredie, v ktorom sa nachádzajú, sa vyznačuje extrémnou dynamikou, heterogenitou a zložitosťou. Digitálne stopy môžu byť roztrúsené v rôznych priestoroch, pričom ich ochrana dosahuje vysokú úroveň. Automatická identifikácia a spracovanie sú možné vďaka špecializovaným nástrojom, avšak kvalifikovaní páchatelia dokážu stopy efektívne odstraňovať. Napriek tomu je však možné čiastočné alebo úplné obnovenie zničených digitálnych stôp, pričom ich originalita zostáva zachovaná.[19]

5 ROLA DIGITÁLNYCH STÔP PRI ROZPOZNÁVANÍ DEZINFORMÁCIÍ

Digitálne stopy vznikajú pri každej interakcii v online priestore – či už ide o zdieľanie príspevkov, vytváranie falošných účtov alebo využívanie botov na automatizované šírenie obsahu. Ich analýza umožňuje analytikom a forenzným expertom efektívne mapovať sieť dezinformačných aktérov a identifikovať vzory správania.

Na identifikáciu dezinformácií prostredníctvom digitálnych stôp sa využívajú viaceré metódy, ktoré umožňujú sledovanie pôvodu a spôsobu šírenia falošných informácií:

Analýza IP adries a metadát – Pomocou IP adries a súvisiacich metadát možno určiť geografický pôvod dezinformácií a prepojenia medzi jednotlivými účtami. Táto metóda umožňuje identifikovať koordinované kampane a lokalizovať hlavné distribučné centrá dezinformácií.

Analýza webových domén – Registrácia domén a hostingové služby môžu odhaliť spojitosti medzi webovými stránkami šíriacimi dezinformácie. Sledovanie údajov o vlastníkoch domén a prevádzkovateľoch serverov môže odhaliť zdroje falošných správ.

Analýza sociálnych médií – Monitorovanie interakcií na sociálnych sieťach umožňuje odhaliť vzory šírenia dezinformácií. Automatizované boty a falošné účty často používajú opakujúce sa frázy a distribuujú obsah koordinovaným spôsobom.

Zachytenie a analýza škodlivého obsahu – Identifikácia podozrivých odkazov, škodlivých súborov a phishingových kampaní je kľúčová pri rozpoznávaní dezinformačných stratégií.

---

[19] METEŇKO, J., METEŇKOVÁ, M., 2024. Theory of Criminalistics traces and their system. Kriminalistinė pėdsakų teorija ir jų sistema. In*.: Juodkaitė-Granskienė, G., Mozūraitis, G., Kriminalistika ir teismo ekspertologija: Mokslas, studijos, praktika, XX. Criminalistics and forensic expertology: science, studies, practice*. Mykolo Romerio universitetas, Lietuvos teismo ekspertizės centras, Lietuvos kriminalistų draugija, Lenkijos kriminalistų draugija, Vilnius, 2024, s. 41-47.

V praxi boli digitálne stopy úspešne použité na identifikáciu viacerých dezinformačných kampaní:

- Ruské zasahovanie do volieb v USA (2016) – Digitálne analýzy odhalili, že stovky falošných účtov na sociálnych sieťach šírili zavádzajúce informácie s cieľom ovplyvniť voličov.[20]
- Šírenie konšpiračných teórií počas pandémie COVID-19 – Výskumníci analyzovali digitálne stopy spojené s falošnými medicínskymi odporúčaniami a identifikovali hlavné zdroje dezinformácií.[21]
- Manipulácia s verejnou mienkou v Európe – Sledovaním IP adries a registrácií domén boli odhalené siete propagandistických webových stránok spojené s rôznymi geopolitickými záujmami.[22]

Aj keď digitálne stopy poskytujú dôležité nástroje na identifikáciu dezinformácií, existujú aj výzvy, ktoré komplikujú tento proces. Ide najmä o používanie anonymizačných technológií ako VPN, Tor a šifrovanej komunikáccie. Využívanie týchto nástrojov sťažuje sledovanie aktérov dezinformačných kampaní. Ďalším faktorom je automatizácia a umelá inteligencia. Pokročilé modely umelej inteligencie môžu generovať sofistikované falošné správy, ktoré sú ťažšie identifikovateľné. Programy využívajúce generatívnu umelú inteligenciu dokážu rýchlo a efektívne generovať originálny obsah podľa zadania užívateľa. Vysoké riziko predstavujú momentálne deepfake, ktoré sú vysoko presvedčivé, napriek tomu že ide o úplne falošný alebo pozmenený audiovizuálny obsah. Identifikovať hranice medzi realitou a fikciou sa plynutím času stáva čoraz náročnejšie najmä kvôli pokročilým mechanizmom strojového učenia. Poslednou výzvou sú právne a etické obmedzenia. Vyhľadávanie, zaisťovanie a skúmanie digitálnych stôp musí prebiehať v súlade s ochranou osobných údajov a platnými právnymi predpismi.

ZÁVER

Predložený článok – na základe výsledkov výskumu – potvrdzuje kľúčovú hypotézu, že v prostredí hybridných hrozieb predstavujú digitálne stopy, získané prostredníctvom digitálnej forenznej analýzy, jeden z najesenciálnejších nástrojov v boji proti dezinformáciám. Analýza demonštruje, že IP adresy, metadáta obsahu, informácie o registrácii domén a schémy šírenia na sociálnych sieťach nie sú iba pasívnymi dátovými záznamami, ale stávajú sa aktívnym forenzným dôkazom, nevyhnutným pre demaskovanie komplexných a často aj štátmi podporovaných dezinformačných kampaní.

Primárny metodologický prínos tejto práce spočíva v zdôraznení potreby posunu od reaktívneho overovania faktov (fact-checking) ku proaktívnej analýze infraštruktúry. Iba dôsledným a včasným mapovaním distribučných mechanizmov, ktoré zahŕňa identifikáciu pôvodných domén, hostingových služieb a kaskádových reťazcov šírenia, je možné efektívne narušiť operačný a ekonomický model dezinformačných aktérov, čím sa minimalizuje riziko ich opakovanej a znovuzrodenej aktivity. Dezinformačné siete sú v konečnom dôsledku rovnako zraniteľné ako akákoľvek iná digitálna infraštruktúra; zraniteľnosť spočíva práve v ich digitálnej stope.

---

[20] MIRGA, T. 2023. Šírenie dezinformácií a organizované ovplyvňovanie verejnej mienky: trolie farmy ako nástroj sociálnej a politickej manipulácie. In *ITlib*. *Informačné technológie a knižnice*. [online]

[21] MINTAL, J. M. 2021 Dezinformácie a konšpiračné teórie v masmediálnom priestore. In *Vojenská osveta*, roč. 79, č. 1-2, s. 72-85;

[22] MIRGA, T. 2023. Šírenie dezinformácií a organizované ovplyvňovanie verejnej mienky: trolie farmy ako nástroj sociálnej a politickej manipulácie. In: *ITlib. Informačné technológie a knižnice.* [online]

Napriek signifikantnému významu digitálnych stôp, táto analýza zároveň reflektuje na akcelerujúce technologické výzvy. Rapídny pokrok v oblasti generatívnej umelej inteligencie (AI) a technológií deepfake predstavuje významnú epistemologickú prekážku, keďže syntetizovaný obsah sa stáva čoraz ťažšie odlíšiteľným od autentického. Súčasne, sofistikované metódy anonymizácie a rozsiahle využívanie proxy sietí trvalo sťažujú určenie geografického pôvodu a reálnej identity páchateľov. Pre vedeckú komunitu je preto imperatívom neustále inovovať digitálne forenzné techniky, prispôsobovať sa dynamike AI-generovaného obsahu a vyvíjať robustné modely atribúcie, ktoré dokážu prekonať súčasné anonymizačné bariéry.

Z týchto zistení vyplýva nevyhnutnosť prijatia holistického prístupu, ktorý presahuje rámec čisto technického riešenia. Na systémovej úrovni je kľúčové komplexné posilnenie legislatívneho rámca s cieľom zvýšiť zodpovednosť online platforiem za obsah šírený prostredníctvom nich, pri plnom rešpektovaní ústavne garantovaných práv. Investície do digitálnej gramotnosti obyvateľstva musia byť doplnené o systémovú medzirezortnú spoluprácu. Táto synergia musí organicky prepojiť expertízu v oblasti kybernetickej bezpečnosti, forenznej informatiky, práva a tvorby politík. Iba prostredníctvom takejto multidisciplinárnej kooperácie je možné dosiahnuť udržateľnú a robustnú odolnosť národného informačného prostredia voči manipulatívnym naratívom, čím sa efektívne a účinne chránia demokratické procesy a sociálna kohézia pred destabilizačnými účinkami hybridných operácií.

ZOZNAM POUŽITEJ LITERATÚRY A ZDROJOV:

BELICA, B. 2024. Vybrané legislatívne možnosti regulácie šírenia dezinformácií. In *Bezpečnosť elektronickej komunikácie : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2024, s. 10-21. ISBN 978-80-8293-021-7.

BENTZEN, N. 2019. Ako odhaliť falošnú správu. [online] [cit. 15.11.2025] Dostupné na: <https://www.europarl.europa.eu/RegData/etudes/ATAG/2017/599386/EPRS_ATA(2017)599386_SK.pdf>.

BURZALA, D. 2024. *Dezinformácie ako „nová hrozba“ pre spoločnosť*. In Bezpečnosť elektronickej komunikácie : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou. Bratislava : Akadémia Policajného zboru, 2024, s. 50-63. ISBN 978-80-8293-021-7.

DUŠEK, J., KAVAN, Š. 2023. Dezinformace jako součást hybridních hrozeb pohledem studentů VŠERS. In *Interpolis*, 2023, s. 7-25. Banská Bystrica : Belianum – Vydavateľstvo Univerzity Mateja Bela, 2023. ISBN 978-80-557-2098-2.

DUŠEK, J., KAVAN, Š. 2024. Dezinformace jako součást hybridních hrozeb – česko-slovenský pohled. In *Auspicia*, 2024, roč. 21, č. 1, s. 7-25. ISSN 2464-7217.

ESET. 2021. *Vaša digitálna stopa: Čo to je a ako sa o ňu starať*. [online]. [cit. 16.11.2025]. Dostupné na internete: https://bezpecnenanete.eset.com/sk/it-bezpecnost/vasa-digitalna-stopa-co-to-je-a-ako-sa-o-nu-starat/

EURÓPSKA KOMISIA. 2022. *Ako nepodľahnúť dezinformáciám? Prinášame päť tipov od odborníkov*. [online]. [cit. 15.11.2025]. Dostupné na internete: https://slovakia.representation.ec.europa.eu/news/ako-nepodlahnut-dezinformaciam-prinasame-pat-tipov-od-odbornikov-2022-05-06sk

HAJDÚKOVÁ, T. 2024. Zdroje informácií alebo dezinformácií. In *Auspicia*, 2024, roč. 21, č. 1, s. 37-49. ISSN 2464-7217.

HAŠANOVÁ, J. 2024. Administratívno-právne aspekty boja proti dezinformáciám. In Dušek, J. a kol.: *Dezinformace ve střední Evropě: vývoj, právní rámce a bezpečnostní dopady v éře*

umělé inteligence a digitálních technologií. České Budějovice : Vysoká škola evropských a regionálních studií, 2024. s. 141-164. ISBN 978-80-7556-143-5.

INTERNETEM BEZPECNE. 2025. Digitální stopa. [online]. [cit. 17.11.2025]. Dostupné na internete: https://www.internetembezpecne.cz/internetem-bezpecne/dobre-vedet/digitalni-stopa/

IVANČÍK, R. – NEČAS, P. 2025. *Hybridné hrozby: Bezpečnostná výzva pre demokratické spoločnosti*. Praha: Leges, 2025. 226 s. ISBN 978-80-7502-823-5.

IVANČÍK, R. 2023. On Disinformation and Propaganda in the Context of the Spread of Hybrid Threats. In *Vojenské reflexie*, 2023, roč. 18, č. 3, s. 38-58. ISSN 1336-9202. DOI: https://doi.org/10.52651/vr.a.2023.3.38-58

IVANČÍK, R. 2024. Dezinformácie ako bezpečnostná hrozba šírená na internete. In *Auspicia*, 2024, roč. 21, č. 1, s. 26-36. ISSN 2464-7217. DOI: 10.36682/a_2024_1_2

IVANČÍK, R. 2025. *Dezinformácie. Teoretické východiská ich skúmania*. Praha: Leges, 2025. 188 s. ISBN 978-80-7502-769-6.

MARWICK, A. – LEWIS, R. 2017. Media Manipulation and Disinformation Online [online] [cit. 13.11.2025] Dostupné na: https://datasociety.net/pubs/oh/DataAndSociety_Media ManipulationAndDisinformationOnline.pdf

METĚNKO, J. a kol. 2004. *Kriminalistické metódy a možnosti kontroly sofistikovanej kriminality*. Bratislava : Akadémia Policajného zboru. ISBN 80-8054-336-4.

METEŇKO, J. a METEŇKOVÁ, M. 2024. Kriminalistický a personálny prístup ku skúmaniu digitálnej stopy. In *Udržitelný rozvoj XV: 20 let členství v EU: Úspěchy, výzvy a perspektivy*, České Budejovice : Vysoká škola evropských a regionálních studií, 2024.

METEŇKO, J., METEŇKOVÁ, M., 2024. Theory of Criminalistics traces and their system. Kriminalistinė pėdsakų teorija ir jų sistema. In.: *Juodkaitė-Granskienė, G., Mozūraitis, G., Kriminalistika ir teismo ekspertologija: Mokslas, studijos, praktika, XX. Criminalistics and forensic expertology: science, studies, practice*. Mykolo Romerio universitetas, Lietuvos teismo ekspertizės centras, Lietuvos kriminalistų draugija, Lenkijos kriminalistų draugija, Vilnius, 2024, s. 41-47. ISSN 2783-7068.

METEŇKO, J., METENKOVÁ, M., 2024. Digital trace as a personal and criminalistics object. In *Security Horizons*. International scientific conference Contemporary security challenges and strengthening the resilience of the countries of southeast europe, roč. 9, č. 1, s. 175-191. DOI 10.20544/ICP.9.1.24., ISSN 2671-3624. [online]. [cit. 16.11.2025]. Dostupné na internete: https://eprints.uklo.edu.mk/id/eprint/10582

MINTAL, J. M. 2021 Dezinformácie a konšpiračné teórie v masmediálnom priestore. In *Vojenská osveta*, roč. 79, č. 1-2, s. 72-85. ISSN 1336-9202.

MIRGA, T. 2023. Šírenie dezinformácií a organizované ovplyvňovanie verejnej mienky: trolie farmy ako nástroj sociálnej a politickej manipulácie. In: *ITlib. Informačné technológie a knižnice*. [online]. [cit. 18.11.2025] s. 42-55. Dostupné na internete: https://itlib.cvtisr.sk/clanky/sirenie-dezinformacii-a-organizovane-ovplyvnovanie-verejnej-mienky-trolie-farmy-ako-nastroj-socialnej-a-politickej-manipulacie/

NOVÁKOVÁ, I. 2022. Boj proti dezinformáciám z pohľadu študentov In *Dezinformácie a právo (úlohy a postavenie bezpečnostných zložiek) : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2020, s. 176-188. ISBN 978-80-8054-965-7.

PORADA, V. a kol. 2019. *Kriminalistika. Technické, forenzní a kybernetické aspekty*. 2. vyd. Plzeň: Aleš Čeněk, 2019. 1205 s. ISBN 978-80-7380-741-2.

SABAYOVÁ, M. 2024. Sebavnímanie odolnosti voči dezinformáciám vo vysokoškolskom prostredí. In *Auspicia*, 2024, roč. 21, č. 1, s. 59-71. ISSN 2464-7217.

VEJVODOVÁ, P. 2019. Information and Psychological Operations as a Challenge to Security and Defence. In. *Vojenské rozhledy* [online]. č. 3, s. 85-86. [cit. 13.11.2025]. Dostupné na internete: https://www.researchgate.net/publication/335947264_Information_and_Psychological_Operations_as_a_Challenge_to_Security_and_Defence

ZACHAR KUCHTOVÁ, J. 2022. Bezpečnosť na sociálnych sieťach. In *Bezpečnosť elektronickej komunikácie : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava: Akadémia Policajného zboru, 2022, s. 237-247. ISBN 978-80-8054-968-8.

ZACHAR KUCHTOVÁ, J. 2024. Šírenie dezinformácií s využitím nástrojov umelej inteligencie. In Dušek, J. a kol.: *Dezinformace ve střední Evropě: vývoj, právní rámce a bezpečnostní dopady v éře umělé inteligence a digitálních technologií*. České Budějovice : Vysoká škola evropských a regionálních studií, 2024. s. 90-107. ISBN 978-80- 7556-143-5.