ACTA FACULTATIS IURIDICAE UNIVERSITATIS COMENIANAE
Tomus XLII
1/2023

CIELE DOKAZOVANIA V KYBERNETICKEJ BEZPEČNOSTI

Ing. Bc. Ivan Makatura, CRISC, CDPSE

Univerzita Komenského v Bratislave, Fakulta managementu
Katedra informačných systémov
ivan.makatura@cybercompetence.sk

Ciele dokazovania v kybernetickej bezpečnosti

Dokazovanie je poznávacia činnosť, ktorou príslušná autorita zisťuje objektívny stav skutočnosti. Získané informácie o skutkovom stave následne môžu slúžiť ako podklad pre ďalšie rozhodovanie štatutárneho zástupcu organizácie, orgánu verejnej moci, prípadne orgánu činného v trestnom konaní, alebo súdu. Získané informácie o skutkovom stave tak treba vnímať, ako základný predpoklad následného spravodlivého rozhodovania konkrétneho subjektu. Vo všeobecnosti platí, že ako dôkaz, môže poslúžiť akákoľvek informácia, ktorá napomôže objasneniu veci, objasneniu objektívneho stavu reality. Informácie vyplývajú z analýzy pôvodných údajov a pri vhodnej interpretácii môžu viesť ku poznaniu. Dôkazné prostriedky v kybernetickom priestore majú špecifický charakter. Ambíciou článku je analýza odlišných a zhodných charakteristík dokazovania s dôrazom na znaleckú činnosť a audit kybernetickej bezpečnosti.

Objectives of proving in cyber security

Proving is a cognitive activity by which the relevant authority ascertains the objective state of the facts. The obtained information about the subject matter can subsequently serve as a basis for further decision-making by the statutory representative of the organization, public authority, or law enforcement body or court. The obtained information about the subject matter should be perceived as an essential prerequisite for the subsequent fair decision-making of a specific subject. In general, any information that helps to clarify the matter, to clarify the objective state of reality, can serve as evidence. Any information results from the analysis of the original data and, with appropriate interpretation, can lead to knowledge. Evidence in cyberspace has a particular nature. The

article aims to explain different and similar characteristics of evidence emphasizing judicial expert's activities and cyber security audits.

Ziele der Beweis Prozess in der Cyber-Sicherheit

Exekution von forensischen Beweismitteln ist eine kognitive Fähigkeit, mit der die Behörde die Fakten einer Falle zu ermitteln. Die erhaltenen Informationen über den Sachverhalt können anschließend als Grundlage für die weitere Entscheidungsfindung durch das gesetzliche Organ, die öffentliche Behörde oder die Strafjustizbehörde oder das Gericht dienen. Die erhaltenen Informationen sind als notwendige Voraussetzung für die spätere faire Entscheidungsfindung durch das befugte Entscheidungsgremium anzusehen. Als Beweismittel können grundsätzlich alle Informationen dienen, die zur Klärung des Sachverhalts, zur Klärung des objektiven Tatbestandes beitragen. Die Informationen resultieren aus der Analyse der Originaldaten und können bei richtiger Interpretation zur Erkenntnis beitragen. Beweise im Cyberspace haben eine spezifische Natur. Das Ziel des Artikels ist es, die Unterschiede und Ähnlichkeiten von Expertenbeweisen mit Schwerpunkt auf forensischen Aktivitäten und Cyber-Sicherheitsaudits zu identifizieren.

Kľúčové slová: kybernetická bezpečnosť, audit; znalec, digitálna stopa, dokazovanie, dôkazné prostriedky

Keywords: cybersecurity, audit, expert witness, digital footprint, proving, evidence

Stichworte: Kyber-Sicherheit, Rechnungsprüfung, forensischer Experte, digitaler Fußabdruck, der Beweisprozess, Beweise

Úvod

Cieľom článku je prostredníctvom porovnania charakteristík procesov dokazovania v znaleckej činnosti a procesov dokazovania pri výkone auditu kybernetickej bezpečnosti zhodnotiť princípy akvizície a spracúvania digitálnych stôp ako potenciálnych dôkazov pre objektívne určenie stavu skutočností v kybernetickom priestore.

Autor sa vo vlastnej praxi znalca zapísaného v Zozname znalcov, tlmočníkov a prekladateľov Ministerstva spravodlivosti Slovenskej Republiky v znaleckom odvetví bezpečnosť informačných systémov stretol s častým s nepochopením problematiky digitálnych stôp zo strany orgánov činných v trestnom konaní a súdov. Mnohokrát si už v čase zberu a získavania stôp subjekty práva zamieňajú významy pojmov. V praxi sa už vyskytli reálne prípady, keď boli vykonané také aktivity, ktoré znemožnili ďalšie použitie získaných informácií v dôkaznom konaní.

Zároveň platí, že kým pre výkon auditu kybernetickej bezpečnosti sú metodikou určené postupy, pre znalectvo v elektrotechnike neexistuje právne záväzné vymedzenie postupov pre identifikáciu, zber, získavanie a uchovávanie digitálnych dôkazov. Aplikovaná je iba dobrá prax, založená na veľmi špecifických zručnostiach, aktuálne dostupných znalostiach a najmodernejších metódach a postupoch (ang. „state of the art“).

V práci bola použitá metodika empirického výskumu a následného porovnania skúmaných procesov z hľadiska ich vyspelosti, s ohľadom na paradoxy spôsobené právnymi a technickými zvláštnosťami skúmaných činností.

Pre opisovanú tematiku sú výrazy „stopa“ a „dôkaz“ kľúčovými termínmi.

Pojem „dôkazy“ sa v kontexte kybernetického priestoru vyskytuje v dvoch procesoch: prvým z nich je výkon znaleckej činnosti podľa zákona č. 382/2004 Z. z. o znalcoch, tlmočníkoch a prekladateľoch a o zmene a doplnení niektorých zákonov[1], druhým je výkon auditu kybernetickej bezpečnosti podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov[2] . Oba tieto procesy majú množstvo porovnateľných, ale aj niekoľko zásadne odlišných charakteristík.

O čom všetkom je možné v kybernetickom priestore získať dôkazy? Kto každý a za akým účelom môže dôkazy získavať? Kto je zvyčajným prijímateľom získaných potenciálnych dôkazov v oblasti kybernetickej bezpečnosti?

Vo vyhláške Národného bezpečnostného úradu č. 493/2022 Z. z. o audite kybernetickej bezpečnosti[3] sa referencia na dôkazy objavuje na niekoľkých miestach. Podstatným v tejto súvislosti je ustanovenie § 1 ods. 7 písm. g) podľa ktorého *pri výkone auditu sa zbierajú, sústreďujú a vyhodnocujú **dôkazy** o zisteniach auditu* a ustanovenie § 2 ods. 1, podľa ktorého *v záverečnej správe o výsledkoch auditu sa hodnotí výsledok auditu a uvedú sa **dôkazy**, ktoré sa viažu k jednotlivým zisteniam auditu*. Bolo by však nekorektné tvrdiť, že problematické použitie termínu „dôkaz“ v kontexte auditu, bolo zavedené až vyhláškou č. 493/2022 Z. z. o audite kybernetickej bezpečnosti.[3] Výraz „auditný dôkaz“ je totiž bežne používaný aj v iných právnych predpisoch a desiatky rokov je aplikovaný prostredníctvom medzinárodnej dobrej praxe auditu všeobecne (napríklad v účtovnom alebo finančnom audite).

---

[1] Zákon č. 382/2004 Z. z. o znalcoch, tlmočníkoch a prekladateľoch a o zmene a doplnení niektorých zákonov.

[2] Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

[3] Vyhláška Národného bezpečnostného úradu č. 493/2022 Z. z. o audite kybernetickej bezpečnosti.

Potrebu opatrného používania termínu dôkaz podčiarkuje aj medzinárodná norma ISO/IEC 27037:2012 *Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence*[4], ktorá je nateraz jediným technickým predpisom, poskytujúcim usmernenia pre konkrétne činnosti pri nakladaní s digitálnymi dôkazmi a uchovávaním informácií, ktoré môžu mať potenciálnu dôkaznú hodnotu. Technická norma ISO/IEC 27037:2012 je v súčasnosti v procese prevzatia do sústavy Slovenských technických noriem. Norma v celom svojom texte používa výhradne výraz „potenciálny dôkaz", zjavne v úmysle ponechať prípustnosť dôkazu na rozhodnutí štatutárneho zástupcu organizácie, orgánu verejnej moci, orgánu činného v trestnom konaní alebo súdu.

Článok sa venuje vysvetleniu rozdielov medzi pojmami stopa a dôkaz, objasneniu špecifík digitálnych stôp a v základnom rozsahu aj princípom získavania digitálnych stôp a manipulácie s digitálnymi stopami. V ďalšej časti opisuje základné princípy znalectva v elektrotechnike a forenzných vied v kybernetickej bezpečnosti, vrátane pomenovania zainteresovaných strán v digitálnej forenznej analýze. Hypoteticky definuje audit kybernetickej bezpečnosti ako dôkazný prostriedok. Následne sú opísané metódy získavania auditných dôkazov a možné chyby v auditoch a znaleckých posudkoch tak, aby po diskusnej časti, v ktorej sú porovnávané zhodné a rozdielne charakteristiky procesov dokazovania v znaleckej činnosti a pri výkone auditu kybernetickej bezpečnosti, bolo možné dospieť k racionálnym záverom.

1. Stopa a dôkaz

Pojem DÔKAZ je pre ďalší opis súvisiacich procesov nevyhnutné odlíšiť od pojmu STOPA a to napriek tomu, že z etymologického hľadiska sú významy oboch slov podobné:

> stopa -y stôp ž. – zvyšok po niečom (po deji, veci ap.), pozostatok, znak: s. farby, s. po údere, s-y vojny, s-y utrpenia (na tvári); odb. zvuková s. (na magnetofónovej páske) záznam, niesť s-y niečoho mať znaky niečoho; prísť niekomu, niečomu na s-u vypátrať; ísť v s-ách niekoho nasledovať (príklad); zmiznúť bez s-y stratiť sa; ani s-y (niet po ňom, po tom) a) stratil(o) sa b) niet ho;[5]

[4] ISO/IEC 27037:2012 Informačné technológie – Bezpečnostné metódy – Návod na identifikáciu, zber, získavanie a uchovávanie digitálnych dôkazov.

[5] KAČALA, J. – PISÁRČIKOVÁ, M. – POVAŽAJ, M. a kol. *Krátky slovník slovenského jazyka* 4. dopl. a upr. vyd. Bratislava : Veda 2003. 985 s. ISBN 80-224-0750-X.

dôkaz-u m. – 1. fakt potvrdzujúci istú mienku: presvedčivý d.; priniesť d. 2. dosvedčenie, svedectvo, podať d. o niečom dokázať niečo; dôkazný, dôkazový príd.: d-ový materiál.[5]

Podľa jednej z mnohých definícií, *stopa je akákoľvek zmena v materiálnom prostredí alebo vo vedomí človeka, ktorá príčinne alebo aspoň miestne a časovo, súvisí s vyšetrovanou udalosťou, obsahuje kriminalisticky alebo trestnoprávne relevantnú informáciu, je zistiteľná, zaistiteľná a využiteľná pomocou dostupných kriminalistických, prírodovedných a technických metód, prostriedkov a postupov*.[6]

V prípade, ak sa dajú nájsť informácie o stope v pôvodnom zdroji a tieto informácie sú relevantné pre skúmané skutočnosti, potom je možné považovať ich za potenciálny dôkaz. Takýto potenciálny dôkaz môže, ale nemusí byť spoľahlivý, pretože informácia, ktorá na prvý pohľad vyzerá spoľahlivo, môže byť nesprávna. A naopak – zdroj, ktorý sa zdá byť nekvalitným, môže v skutočnosti obsahovať správne informácie. Žiadnu informáciu nie je možné prijať bez kritického skúmania. Každá informácia si žiada, aby bola použitá len ako stopa k dôležitejšiemu a komplexnejšiemu poznaniu skutočnosti.[7]

Informačný obsah tej ktorej stopy nemusí vždy vykazovať dôkazovú relevanciu. Stopa je indikáciou, ktorá môže viesť k pochopeniu skutkového stavu a vykonaniu potenciálneho dôkazu pomocou dôkazných prostriedkov. Dôkazy sú získané, agregované informácie o stopách, ktoré môžu byť použité na podporu tvrdení alebo aj na ich vyvrátenie. Z tohto pohľadu všetko, čo považujeme za relevantné pre konkrétny problém, je zároveň stopou a potenciálnym dôkazom súčasne.

Ak opisujeme vnímanie výrazu dôkaz v konaní pred súdom, rovnako Trestný poriadok[8] v § 119 ods. 2 ako aj Civilný sporový poriadok v § 187 ods. 1[9] majú takmer totožné definície: za dôkaz môže slúžiť všetko, čo môže prispieť k náležitému objasneniu veci a čo sa získalo zákonným spôsobom, z dôkazných prostriedkov.

Technická norma[4] považuje za digitálne dôkazy informácie alebo údaje, uložené alebo zasielané v binárnej forme, na ktoré sa možno opierať v dôkaznom konaní. Rôzne zariadenia sú spôsobilé generovať alebo uchovávať dáta, ktoré môžu byť využiteľné ako zdroj elektronických dôkazov v trestnom konaní. V závislosti od zdroja môžu mať také-

[6] STRAUS, Jiří – VAVERA, František. *Slovník kriminalistických pojmů a osobností.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2010. ISBN 978-80-7380-258-5.

[7] SHOWN MILLS Elizabeth. *Is It Evidence or ‚Just a Clue'?* blog post, QuickTips: The Blog @ Evidence Explained. 15 September 2018. [online].

[8] Zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov.

[9] Zákon č. 160/2015 Z. z. Civilný sporový poriadok v znení neskorších predpisov.

to dáta rôzny charakter a musia sa k nim pri dokazovaní rôzne pristupovať tak z technického, ako aj procesného hľadiska.[10]

Dôkazným prostriedkom sa rozumie nástroj, prostredníctvom ktorého sú získané poznatky o predmete dokazovania. Dôkazným prostriedkom podľa Civilného sporového poriadku je najmä výsluch strany, výsluch svedka, listina, odborné vyjadrenie, znalecké dokazovanie a obhliadka. Dôkaznými prostriedkami podľa Trestného poriadku sú najmä výsluch obvineného, svedka, znalca, posudky a odborné vyjadrenia, previerka výpovede na mieste, rekognícia, rekonštrukcia, vyšetrovací pokus, obhliadka, veci a listiny dôležité pre trestné konanie, oznámenie, informácie získané použitím informačno-technických prostriedkov, alebo prostriedkov operatívno-pátracej činnosti.

Pod pojmom dôkazný prostriedok je v zásade možné rozumieť procesnú činnosť (úkony), pomocou ktorej sa získavajú poznatky, slúžiace k spoznaniu skutočnosti, ktorá má byť zistená. Dôkaz je potom výsledok činnosti orgánov činných v trestnom konaní a súdu pri dokazovaní.[11] Rozumie sa ním priamy poznatok, ktorý bol získaný z dôkazného prostriedku pri dokazovaní.

Hoci základné procesné predpisy pojmy dôkaz a dôkazný prostriedok nerozlišujú, teória trestného práva považuje dôkaz za informáciu o veci a dôkazný prostriedok ako zdroj tejto informácie. Dôkazný prostriedok tak možno vymedziť ako „zdroj, z ktorého orgán činný v trestnom konaní dôkazy čerpá (výpovede osôb, veci)“[12.] Za elektronický dôkazný prostriedok je teda možné považovať všetko, čo môže slúžiť ako zdroj relevantnej informácie a čo je uchované v elektronickej podobe – predovšetkým dáta.[13]

Problematika vzťahu dát a informácií podrobnejšie pojednáva teória tzv. informačnej pyramídy. Hierarchia dát, informácií, vedomostí a poznania alebo tiež tzv. DIKW pyramída (z angl. „Data-Information-Knowledge-Wisdom“) spája vzťahy logicko-konceptuálnych objektov ako štyroch vrstiev hypotetickej pyramídy. Teória DIKW sa široko pou-

---

[10] POLČÁK, Radim – PÚRY, František – HARAŠTA, Jakub a kol. *Elektronické důkazy v trestním řízení.* 1. vyd. Brno : Masarykova univerzita, Právnická fakulta, 2015. 253 s. Spisy Právnické fakulty Masarykovy univerzity, řada teoretická, Edice Scientia č. 542. ISBN 978-80-210-8073-7. str. 83.

[11] JELÍNEK, Jiří. *Trestní zákoník a trestní řád: s poznámkami a judikaturou.* 7. aktualizované vydání podle stavu k 1.10.2017. Praha: Leges, 2017, s 784.

[12] CÍSAŘOVÁ, D. – FENYK, J. – GŘIVNA, T. et al. *Trestní právo procesní.* 5. vyd. Praha: ASPI, 2008, s. 284.

[13] POLČÁK, Radim – PÚRY, František – HARAŠTA, Jakub a kol. *Elektronické důkazy v trestním řízení.* 1. vyd. Brno : Masarykova univerzita, Právnická fakulta, 2015. 253 s. Spisy Právnické fakulty Masarykovy univerzity, řada teoretická, Edice Scientia č. 542. ISBN 978-80-210-8073-7. str. 94.

žíva v rámci informačnej vedy a znalostného manažmentu. Podstatou tejto konštrukcie je dokázaný fakt, že dáta bez konkrétneho kontextu a bez vlastníka sú de facto len fyzikálnymi hodnotami. Informácie sú pochopením vzťahu medzi časťami dát. Následnú hodnotu získavajú až interpretované informácie, z ktorých vyplývajú konkrétne čiastkové vedomosti. Vrcholom tejto pyramídy je pochopenie významu a súvislostí. Teóriu DIKW opisujú mnohí teoretici z odboru informačného manažmentu.[14] [15] Ako prvý s konceptom hierarchie informácií pozostávajúcej zo „signálov, správ, informácií a vedomostí" prišiel anglicko-americký ekonóm a pedagóg Kenneth Boulding.[16] Prvým autorom, ktorý rozlišoval medzi údajmi, informáciami a vedomosťami a tiež použil termín znalostný manažment, bol americký pedagóg Nicholas L. Henry v roku 1974.[17]

Každá vyššia úroveň v informačnej pyramíde poskytuje dodatočné odpovede ku počiatočným dátam, čím im pridáva hodnotu. Čím viac obohatíme pôvodné dáta o kontext, tým viac vedomostí a následne objektívnych poznatkov o stave skutočnosti z nich získame. Graficky sa táto postupnosť v poznaní stavu skutočností dá zobraziť nasledovne:

Obr. 1 Informačná pyramída
(Zdroj: Vlastné spracovanie)

[14] FRICKÉ, Martin. *Data-Information-Knowledge-Wisdom (DIKW) Pyramid, Framework, Continuum.* V Encyclopedia of Big Data, 1–4. Cham: Springer International Publishing, 2018. https://doi.org/10.1007/978-3-319-32001-4_331-1. ISBN: 978-3-319-32001-4.

[15] ALLEN, Greenwood. *Hierarchy of Knowledge – from Data to Wisdom.* (2017). International Journal of Current Research in Multidisciplinary (IJCRM) ISSN: 2456-0979.

[16] BOULDING, Kenneth. *Notes on the Information Concept.* Exploration. Toronto. 6: 103–112. CP IV, 1955. str. 21–32.

[17] HENRY, Nicholas L. *Knowledge Management: A New Concern for Public Administration*. Public Administration Review, vol. 34, no. 3, 1974, str. 189–96. JSTOR 974902. https://doi.org/10.2307/974902.

Praktickú platnosť teórie informačnej pyramídy v dôkaznom konaní potvrdzuje aj konštatovanie prof. Polčáka: „*dáta ako elektronické dôkazné prostriedky možno chápať ako nespracované fakty a údaje bez pridanej hodnoty interpretácie či analýzy. Samotné dôkazy, teda informácie, sú dáta, ktoré boli interpretované tak, aby mali nejaký zmysel pre ich spracovateľov*“.[18]

V konaní pred súdom, ak nie je spôsob vykonania dôkazu predpísaný, určí ho súd. Dôkazy hodnotí súd podľa svojej úvahy v súlade so zákonnými princípmi, pričom žiaden dôkaz nemá ustanovenú menšiu či väčšiu zákonnú silu.

Dôkazy založené na digitálnych stopách je možné použiť v odlišných scenároch, pričom každý má odlišnú váhu v závislosti od kvality stôp, aktuálnosti analýzy a nákladov potrebných na získavanie takýchto digitálnych stôp.

Digitálne dôkazy sú informácie alebo údaje, uložené alebo zasielané v binárnej forme, na ktoré sa možno opierať v dôkaznom konaní (v kontexte procesných predpisov), alebo v záverečnej správe určitého typu posúdenia (napr. v kontexte auditu kybernetickej bezpečnosti).

2. Digitálne stopy

Digitálna stopa (niekedy tiež „digitálny tieň“) označuje jedinečnú množinu vystopovateľných digitálnych aktivít, činností, príspevkov a komunikácie na internete a/alebo pomocou zariadení informačných a komunikačných technológií.

Digitálne stopy možno klasifikovať ako pasívne alebo aktívne.

Pasívna digitálna stopa – dáta, ktoré používateľ zanecháva nechtiac pri online činnostiach (napr. IP adresa, geografická lokácia zariadenia, cookie a pod.).

Aktívna digitálna stopa – údaje, ktoré používateľ odosiela do kybernetického priestoru úmyselne, s istým zámerom (napr. e-maily, príspevky na sociálnych sieťach, obsah chatov a SMS správ, história internetových prehliadačov, história vyhľadávania, metadáta fotografií, záznamy o používaní platobných kariet a mnohé iné).

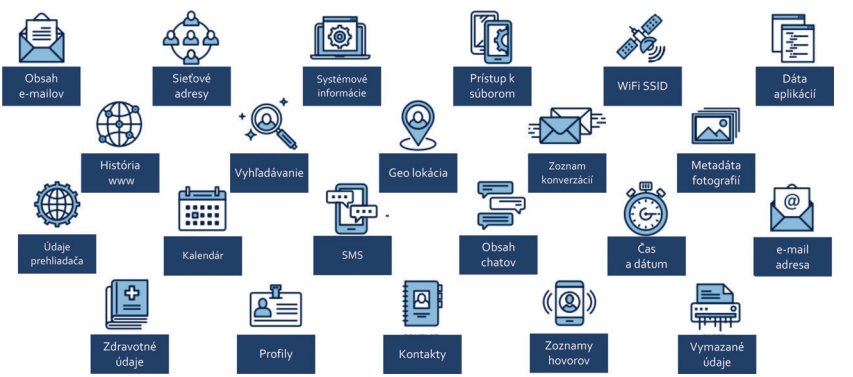
Digitálne stopy sú reprezentované vo fyzickej aj logickej forme.

---

[18] POLČÁK, Radim – PÚRY, František – HARAŠTA, Jakub a kol. Elektronické důkazy v trestním řízení. 1. vyd. Brno : Masarykova univerzita, Právnická fakulta, 2015. 253 s. Spisy Právnické fakulty Masarykovy univerzity, řada teoretická, Edice Scientia č. 542. ISBN 978-80-210-8073-7. str. 94.

– Fyzická forma zahŕňa zobrazenie údajov na rozhraní konkrétneho zariadenia, alebo údajov na fyzických dátových médiách.
– Logická forma sa týka virtuálneho zobrazenia a interpretácie údajov.

Na nasledujúcej ilustrácii je vyobrazených niekoľko vybraných príkladov zdrojov digitálnych stôp.



Obr. 2 Príklady zdrojov digitálnych stôp
(Zdroj: Vlastné spracovanie)

3. Zaobchádzanie s digitálnymi stopami

Slovenský právny poriadok požiadavky na zaobchádzanie s digitálnymi stopami explicitne nedefinuje a neustanovuje žiadne špecifické nároky na postupy, obsah analýz, alebo spôsob vykonania digitálnych stôp ako potenciálnych dôkazov. Po právnej stránke sa kladie dôraz najmä na zákonne získané dôkazy, resp. prípustné dôkazy. Platí, že nezákonný dôkaz je súčasne neprípustný. Prípustnosť sa mnohokrát označuje aj ako zákonnosť, ide však o dva odlišné termíny. „*Neprípustnosť je považovaná za širší pojem, ktorý zahŕňa nielen neprípustnosť vyplývajúcu z nezákonného dôkazu, ale i neprípustnosť danú prameňom dôkazu a neprípustnosť z formálneho dôvodu časovej preklúzie predloženia dôkazov procesnými stranami na súd*.[19] Nedostatky v dokazovaní, spočívajúce v nesprávnom vyhodnotení otázky zákonnosti a prípustnosti

[19] ŠIMOVČEK, I. Prípustnosť dôkazov v trestnom konaní. In Teoretické a praktické problémy dokazovania. Eurokódex, 2008, s. 255. EAN 9788089363223.

určitého dôkazu, tak môžu bezprostredne viesť k oprávnenému spochybneniu výsledkov dokazovania.[20]

Zaujímavé je tiež sledovať vývoj názorov na vykonanie digitálnych dôkazov, a to ako listinných, resp. vecných. Z technického pohľadu sú úsmevné tvrdenia, že napríklad vytlačená správa elektronickej pošty (bez zachovania obsahu metadát z tzv. SMTP hlavičky), alebo predloženie veci, napr. prenosného média (bez dôveryhodnej interpretácie na ňom uloženého obsahu) sú digitálnymi dôkazmi. Získaná digitálna stopa je podľa platnej právnej úpravy v dôkaznom konaní vykonaná ako vecný dôkaz.

Právna úprava procesu dokazovania však nie je úplne vyhovujúca, pretože neobsahuje napr. jasne stanovené limity pre prípustnosť alebo neprípustnosť určitých dôkazných postupov a prostriedkov, ale tie spravidla vymedzuje len judikatúra súdov.[21]

Usmernenia pre špecifické činnosti pri zaobchádzaní s digitálnymi stopami poskytuje už spomínaná medzinárodná technická norma ISO/IEC 27037:2012 *Informačné technológie – Bezpečnostné metódy – Návod na identifikáciu, zber, získavanie a uchovávanie digitálnych dôkazov* [4], vydaná medzinárodnou štandardizačnou organizáciou.

Rozlišujú sa dve základné metódy, akými je možné zaobstarať digitálne stopy:

- zber (alebo tiež zhromažďovanie) – je taký proces nadobudnutia, v ktorom sú zariadenia a fyzické položky, ktoré môžu obsahovať potenciálne dôkazy, odstránené z pôvodného umiestnenia (napr. z pracoviska podozrivého) a prenesené do laboratória, alebo do iného kontrolovaného prostredia na neskoršiu analýzu.
- akvizícia (získavanie) – je taký proces nadobudnutia, ktorý zahŕňa vytvorenie kópie digitálnych dôkazov v rámci definovanej množiny (napr. kompletného obsahu úložiska, logického oddielu disku, vybraných súborov, dump pamäte, atď.) a dokumentovanie použitých metód a vykonaných činností pričom produktom akvizície je digitálna kópia potenciálnych dôkazov.

---

[20] MOLITORIS, Peter. Vzťah medzi zákonnosťou a prípustnosťou dôkazov vo veciach správneho trestania. STUDIA IURIDICA Cassoviensia, ročník 6.2018, číslo 1, 33. ISSN 1339-3995.

[21] POLČÁK, Radim – PÚRY, František – HARAŠTA, Jakub a kol. *Elektronické důkazy v trestním řízení.* 1. vyd. Brno : Masarykova univerzita, Právnická fakulta, 2015. 253 s. Spisy Právnické fakulty Masarykovy univerzity, řada teoretická, Edice Scientia č. 542. ISBN 978-80-210-8073-7. str. 81.

Ďalšími súvisiacimi špecifickými činnosťami pri zaobchádzaní s potenciálnymi digitálnymi stopami pred a po ich zaobstaraní sú najmä:

- identifikácia digitálnych stôp – t. j. proces zahŕňajúci vyhľadávanie, interpretáciu kontextu, uznanie a dokumentáciu potenciálnych digitálnych dôkazov,
- uchovanie digitálnych stôp – t. j. proces zachovania a zabezpečenia integrity a/alebo pôvodného stavu potenciálnych digitálnych dôkazov.

Návody uvedené v ISO/IEC 27037 je vhodné dodržiavať pri každom vyšetrovaní, ktorého cieľom je zachovanie integrity, pôvodu a nepopierateľnosti digitálnych stôp a ktorého cieľom je uplatnenie takých metód pri získavaní potenciálnych digitálnych dôkazov, ktoré prispejú k ich prípustnosti v trestnoprávnych, či občianskoprávnych sporoch, či správnych alebo disciplinárnych konaniach, ako aj v iných príslušných prípadoch.

Okrem ISO/IEC 27037 je možné opierať sa aj o iné relevantné de-facto štandardy, vydané rôznymi autoritami, napr. dokument „*ACPO Good Practice Guide for Digital Evidence*“ vydaný Asociáciou policajných veliteľov Spojeného kráľovstva Veľkej Británie a Severného Írska (Association of Chief Police Officers of England, Wales & Northern Ireland). Podobné štandardy sa z obsahového hľadiska a navrhovaných postupov podstatným spôsobom neodchyľujú od medzinárodnej normy ISO/IEC 27037 a sledujú tie isté ciele, resp. sú založené na rovnakých, alebo porovnateľných metódach a mechanizmoch.

Norma ISO/IEC 27037 ani iné spomenuté de-facto štandardy sa však nevzťahujú na spôsob analýzy digitálnych stôp. Analýza a ostatné procesy súvisiace a forenznými vedami a manažmentom digitálnych stôp sú čiastočne opísané v niekoľkých technických normách, najmä:

- ISO 21043-1:2018 *Forensic sciences – Part 1: Terms and definitions* – dokument definuje pojmy používané v sérii noriem ISO 21043.
- ISO 21043-2:2018 *Forensic sciences – Part 2: Recognition, recording, collecting, transport and storage of items* – dokument špecifikuje požiadavky na forenzný proces, najmä rozpoznávanie, evidenciu, zhromažďovanie, prepravu a uchovávanie vecí s potenciálnou forenznou hodnotou. Zahŕňa požiadavky na posudzovanie a skúmanie scén, ale vzťahuje sa aj na činnosti, ktoré sa vyskytujú v zariadení. Obsahuje aj požiadavky na kvalitu.

– ISO/IEC 30121:2015 *Information technology – Governance of digital forensic risk framework* – poskytuje rámec pre prípravu organizácie na digitálne vyšetrovanie pred tým, než k nemu dôjde. Vzťahuje sa na vývoj strategických procesov týkajúcich sa uchovávania, dostupnosti, prístupu a nákladovej efektívnosti zverejňovania digitálnych dôkazov.

Medzinárodná štandardizačná organizácia v súčasnosti pracuje na vývoji niekoľkých ďalších technických noriem, týkajúcich sa digitálnej forenznej analýzy. V štádiu „CD" (ang. „Committee draft) je pracovný návrh textu normy rozoslaný členom komisie, ktorí text následne pripomienkujú prostredníctvom portálu elektronického hlasovania a to až do doby, kým sa nedosiahne konsenzus o technickom obsahu. V súčasnosti sú v štádiu CD nasledovné technické normy:

– ISO/CD 21043-3.2 *Forensic Sciences – Part 3: Analysis*
– ISO/CD 21043-4.2 *Forensic Sciences – Part 4: Interpretation*
– ISO/CD 21043-5.2 *Forensic Sciences – Part 5: Reporting*

Analýza digitálnych stôp je predmetom najlepšej praxe, založenej na veľmi špecifických zručnostiach, ktoré nutne musia zohľadňovať uznávané najmodernejšie metódy a postupy (ang. „state of the art"). Vzhľadom na komplexnosť a rozsah témy nie je analýza digitálnych stôp v možnostiach jediného odborného článku a preto sa táto práca analýze digitálnych stôp nevenuje.

4. Znalectvo a forenzné vedy v kybernetickej bezpečnosti

Forenzia (z lat. „Forensis" – súdne, od „Forum" – verejné priestranstvá, kde sa konali súdy). „Forenzné" znamená „súdne", preto „Forenzia" zvyčajne označuje postupy a vedy, súvisiace s vyšetrovaním a súdnym dokazovaním.

Forenzná veda (alebo skrátene forenzika, ang.: „forensics") je vedný odbor, ktorý sa zaoberá vyšetrovaním, získavaním stôp a dokazovaním bezpečnostného incidentu alebo porušenia práva štátu či pravidiel organizácie.

Digitálna forenzná analýza (DFA) je odbor forenznej vedy, ktorý sa zaoberá:

– získavaním a skúmaním stôp v elektronických zariadeniach,
– dokazovaním kybernetických bezpečnostných incidentov.

Pojem sa rozšíril na skúmanie všetkých zariadení, schopných uchovávať údaje v elektronickej forme, preto sa nejedná už len o analýzu dát v číslicovej forme.

Cieľom forenznej analýzy je zaručiť vykonanie špecifických činností pri zaobchádzaní s potenciálnymi dôkazmi, najmä:

– identifikácia (digitálnych) stôp,
– zber alebo získavanie stôp,
– uchovanie stôp ako potenciálnych dôkazov.

Vyspelosť činností forenznej analýzy následne napomáha zachovať integritu potenciálnych dôkazov prijateľnou metodológiou pri získavaní stôp, ktorá prispeje k ich prípustnosti v právnych a disciplinárnych, či správnych konaniach.

Dobrá prax forenznej analýzy poskytuje všeobecné usmernenia aj pre získavanie iných ako digitálnych stôp, ktoré môžu byť užitočné vo fáze analýzy potenciálnych digitálnych dôkazov (fyzické stopy).

V zmysle zákona č. 382/2004 Z. z. o znalcoch, tlmočníkoch a prekladateľoch[1] sa znaleckou činnosťou rozumie špecializovaná odborná činnosť, vykonávaná za podmienok ustanovených v zákone znalcami pre zadávateľa. Znalec, alebo tiež „súdny znalec" je fyzická osoba alebo právnická osoba, splnomocnená štátom na vykonávanie činnosti podľa zákona, ktorá je zapísaná v zozname znalcov, tlmočníkov a prekladateľov Ministerstva spravodlivosti SR. Znalec je osoba so špeciálnymi odbornými znalosťami, odlišná od procesných strán a orgánov činných v trestnom konaní, ktorá sa priberá za účelom objasnenia konkrétnej skutočnosti dôležitej pre konanie, pokiaľ sa na objasnenie skutočnosti vyžadujú odborné znalosti.

Zoznam znaleckých odborov a odvetví sa ustanovuje v prílohe č. 1 vyhlášky Ministerstva spravodlivosti SR č. 228/2018 Z. z., ktorou sa vykonáva zákon č. 382/2004 Z. z. o znalcoch, tlmočníkoch a prekladateľoch.[22]

Kybernetická bezpečnosť je komplexná disciplína, ktorá si zvyčajne vyžaduje uplatnenie niekoľkých rôznych znaleckých odvetví. Odvetvia v odbore Elektrotechnika relevantné z hľadiska kybernetickej bezpečnosti sú najmä:

– 10 01 00 – Elektro-energetické stroje a zariadenia,
– 10 02 00 – Elektronika,
– 10 04 00 – Riadiaca technika, výpočtová technika (hardvér),
– 10 06 00 – Elektronické komunikácie,
– 10 07 00 – Odhad hodnoty elektrotechnických zariadení a elektroniky,

[22] Vyhláška Ministerstva spravodlivosti SR č. 228/2018 Z. z. ktorou sa vykonáva zákon č. 382/2004 Z. z. o znalcoch, tlmočníkoch a prekladateľoch a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

– 10 08 00 – Nosiče zvukových a zvukovoobrazových záznamov,
– 10 09 00 – Počítačové programy (softvér),
– 10 10 00 – Bezpečnosť a ochrana informačných systémov.

Okrem znaleckého odboru Elektrotechnika môžu byť z iných znaleckých odborov relevantné z hľadiska kybernetickej bezpečnosti nasledujúce znalecké odvetvia:

– 49 20 00 – Kriminalistická informatika,
– 50 01 00 – Ochrana utajovaných skutočností,
– 04 03 00 – Technický stav pozemného navádzacieho zariadenia,
– 05 02 00 – Technický stav zabezpečovacieho zariadenia,
– 06 03 00 – Signalizačné a zabezpečovacie zariadenie,
– 39 11 00 – Mechanické zabezpečovacie systémy,
– 26 01 00 – Priemyselné vlastníctvo.

Obsahové vymedzenie znaleckých odborov a odvetví je uvedené v Prílohe č. 2 vyhlášky č. 228/2018 Z. z.

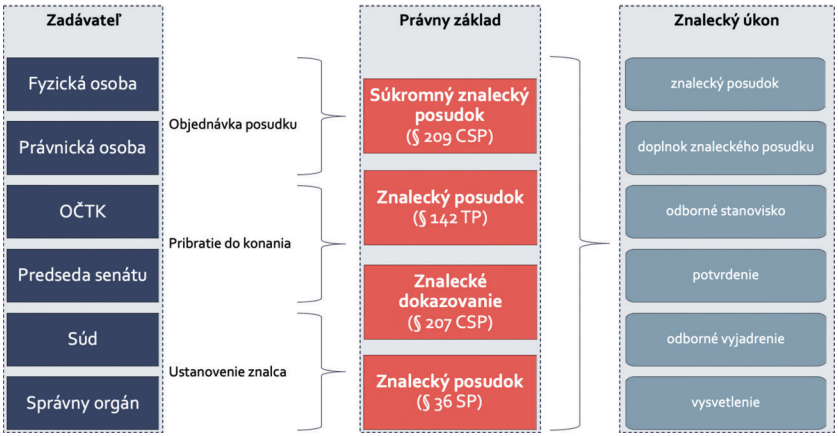
Úlohou znalca je zodpovedať na zadávateľom položené otázky v znaleckom posudku. V zmysle ustanovenia § 145 ods. 2 zákona č. 301/2005 Z. z. Trestný poriadok8 znalec podáva výsledný posudok spravidla písomne, len výnimočne, v jednoduchších prípadoch, možno dovoliť, aby ho nadiktoval do zápisnice o výsluchu. Ak znalec spracoval posudok písomne, stačí, aby sa pri výsluchu naň odvolal. Znalec nie je oprávnený riešiť právne otázky, robiť právne závery, ani hodnotiť vykonané dôkazy.

Právnym základom pre zadanie znaleckého úkonu môže byť:

– súkromný znalecký posudok, predložený stranou bez toho, aby znalecké dokazovanie nariadil súd, v zmysle § 209 ods. 1 zákona č. 160/2015 Z. z. Civilný sporový poriadok[9],
– znalecké dokazovanie, nariadené súdom, ktorý ustanoví znalca, v zmysle § 207 ods. 1 zákona č. 160/2015 Z. z. Civilný sporový poriadok[9],
– znalecký posudok, na základe ustanovenia znalca zo strany správneho orgánu, v zmysle § 36 ods. 1 zákona č. 71/1967 Zb. o správnom konaní (správny poriadok)[23]
– znalecký posudok, na základe pribratia znalca orgánom činným v trestnom konaní alebo predsedom senátu, v zmysle § 142 ods. 1 zákona č. 301/2005 Z. z. Trestný poriadok.[8]

Možní zadávatelia znaleckého úkonu pre znalca, právne základy znaleckých úkonov a typy znaleckých úkonov sú zobrazené v nasledujúcej schéme.

[23] Zákon č. 71/1967 Zb. o správnom konaní (správny poriadok) v znení neskorších predpisov.



Obr. 3 Znalecké úkony
(Zdroj: Vlastné spracovanie)

Úlohy, ktoré má znalec riešiť z hľadiska svojej odbornosti, sa mu určia spravidla v objednávke znaleckého posudku, alebo v uznesení o pribratí, či ustanovení znalca, a to formou otázok.

Ak ide o objasnenie skutočnosti obzvlášť zložitej, v zmysle § 142 ods. 1 Trestného poriadku[8], orgán činný v trestnom konaní, alebo súd, priberie do trestného konania na podanie znaleckého posudku dvoch znalcov, alebo podľa § 143 Trestného poriadku predovšetkým znaleckú organizáciu, špecializovanú na činnosť, ktorá je obsahom znaleckého posudku. V tejto súvislosti je vhodné spomenúť, že ak sa pribralo viac znalcov, ktorí dospeli po vzájomnej porade k súhlasným záverom, stačí, ak podá posudok ten z nich, ktorého sami určili. Ak sa závery znalcov odlišujú, podá posudok samostatne každý z nich.

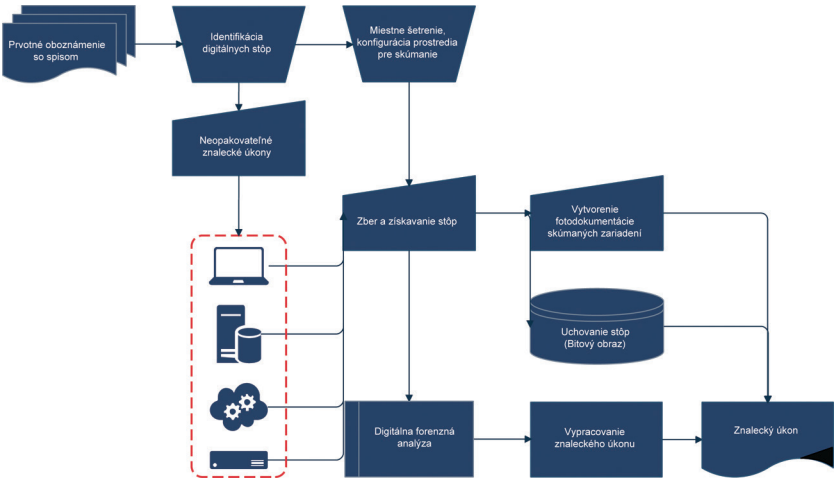
V zmysle § 147 ods. 1 Trestného poriadku[8], vo výnimočných a obzvlášť závažných prípadoch, vyžadujúcich osobitné vedecké posúdenie, alebo na preskúmanie posudku znalca, môže orgán činný v trestnom konaní alebo súd pribrať na podanie znaleckého posudku znalecký ústav.

Proces znaleckého skúmania je možné zobraziť aj graficky, formou schémy na obr. č. 3. V schéme nie sú zachytené všetky fázy životného cyklu znaleckého úkonu, špecifické úkony, týkajúce sa akvizície volatilných údajov, ani procesné úkony, týkajúce sa dôkazných prostriedkov a ďalšej manipulácie s posudkom. Schéma slúži len na znázornenie základných krokov v znaleckých úkonoch.

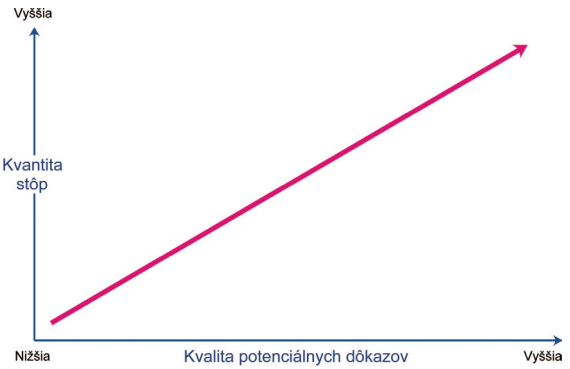
Práve znalci zapísaní v odboroch relevantných pre kybernetickú bezpečnosť pri svojej činnosti využívajú metódy digitálnej forenznej

analýzy. V každom znaleckom úkone musí byť opísaný postup a musí byť zabezpečená jeho preskúmateľnosť. To sú spoločné požiadavky tak pre znalecké úkony, ako aj pre audity.

Na rozdiel od auditu, pri ktorom je prípustné tzv. vzorkovanie (t. j. proces výberu menej ako 100 % položiek z celkového dostupného základného súboru na získanie a vyhodnotenie dôkazov o nejakej vlastnosti základného súboru) – viď. ďalej, v znalectve je kvantita získaných stôp v priamej úmere ku kvalite dôkazného prostriedku.



Obr. 4 Proces znaleckého skúmania
(Zdroj: Vlastné spracovanie)



Obr. 5 Vzťah kvantity stôp a kvality potenciálnych dôkazov
(Zdroj: Vlastné spracovanie)

Získanie menšieho množstva identifikovaných stôp nutne vedie ku nižšej interpretačnej hodnote dôkazného prostriedku.

5. Zainteresované strany v digitálnej forenznej analýze

Stranami v digitálnej forenznej analýze sú zadávatelia posudkov, osoby, ktoré sú zodpovedné za identifikáciu, zber, získanie a uchovanie potenciálnych digitálnych dôkazov a osoby, ktoré môžu byť prijímateľmi potenciálnych digitálnych dôkazov.

Za identifikáciu, zber, získanie a uchovanie potenciálnych digitálnych dôkazov zodpovedajú v pracovno-právnych a obchodných vzťahoch najmä:

- špecialisti informačnej bezpečnosti,
- špecialisti na riešenie incidentov,
- manažéri informačnej a kybernetickej bezpečnosti,
- zamestnanci forenzných laboratórií,

a vo vyšetrovaniach a konaniach pred súdom najmä:

- forenzní technici (z angl. „Digital Evidence First Responders" – DEFR),
- forenzní špecialisti (z angl. „Digital Evidence Specialists – DES),
- znalci zapísaní v príslušnom odvetví a znaleckom odbore.

Prijímateľmi potenciálnych digitálnych dôkazov sú väčšinou účastníci konania, avšak vo všeobecnosti to môžu byť akékoľvek osoby, ktoré potrebujú určiť a preukázať objektívny stav skutočností, prostredníctvom spoľahlivých dôkazov.

V pracovno-právnych a obchodných sú prijímateľmi najmä:

- štatutárni zástupcovia organizácií,
- zamestnanci právnych oddelení,
- fyzické alebo právnické osoby, zastupujúce na základe splnomocnenia v zmysle ustanovení § 31 a nasl. zákona č. 40/1964 Zb. Občiansky zákonník,[24]
- špecialisti pre riešenie podvodov,
- špecialisti ľudských zdrojov,
- interní audítori.

Vo vyšetrovaniach, správnych konaniach a konaniach pred súdom sú to najmä:

[24] Zákon č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov.

– orgány činné v trestnom konaní (v zmysle §10 ods. 1 Trestného poriadku je orgánom činným v trestnom konaní prokurátor a policajt),
– orgány verejnej moci,
– súdy,
– obhajcovia, advokáti,
– sporové strany (strany, účastníci konania), poškodený, obvinený, obžalovaný, ďalšie osoby so spôsobilosťou konať pred súdom (samostatne alebo za osobu, ktorá úplne alebo čiastočne nemá spôsobilosť samostatne konať pred súdom) (zákonný zástupca, opatrovník, orgány starostlivosti o mládež, a ďalší).

6. Audit ako dôkazný prostriedok

Audit je systematický, nezávislý a zdokumentovaný proces získavania záznamov, konštatovaní faktov, alebo iných dôležitých informácií a ich objektívneho posudzovania s cieľom určiť rozsah, v akom sa splnili určené požiadavky. To platí aj pre audit kybernetickej bezpečnosti, vykonávaný podľa § 29 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti[2].

Termín auditné dôkazy podľa technickej normy STN EN ISO 19011:2019[25] je významovo podobný definícii dôkazu uvedenej v § 119 ods. 3 zákona č. 301/2005 Z. z. Trestný poriadok[8]. Podľa čl. 3.9 STN EN ISO 19011: 2019 *Návod na auditovanie systémov manažérstva* (ISO 19011:2018)[16] auditné dôkazy sú záznamy, konštatovania skutočnosti, alebo ďalšie informácie, ktoré sa týkajú kritérií auditu a sú verifikovateľné. Podľa Trestného poriadku[8] za dôkaz môže slúžiť všetko, čo môže prispieť na náležité objasnenie veci a čo sa získalo z dôkazných prostriedkov podľa tohto zákona alebo podľa osobitného zákona.

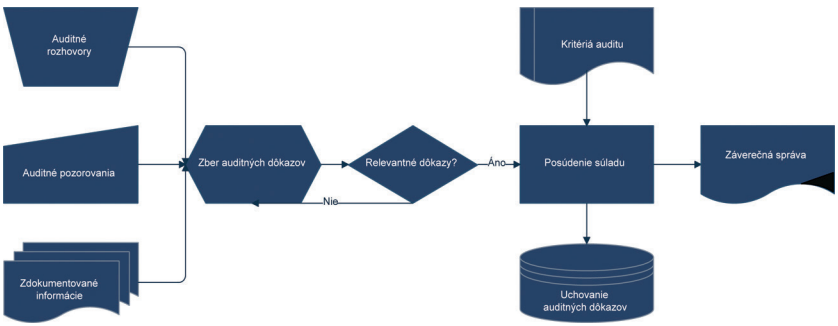
Cieľom auditu je posúdiť súlad a spracovať záverečnú správu o výsledkoch auditu, v ktorej sú zhrnuté zistenia auditu a konštatovaná miera súladu s kritériami auditu. Z toho vyplýva, že kým znalec skúma neznáme prostredie a v procese digitálnej forenznej analýzy sa snaží identifikovať, zozbierať, získať a uchovať digitálne stopy, audítor skúma skutkový stav jej porovnávaním s vopred definovanými kritériami. Pri audite, na rozdiel od znaleckého úkonu, musí existovať vopred definovaná špecifikácia.

Podľa § 29 ods. 1 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti[2] *auditom kybernetickej bezpečnosti sa rozumie overenie plnenia*

[25] STN EN ISO 19011:2019 Návod na auditovanie systémov manažérstva (ISO 19011:2018).

povinností podľa tohto zákona, posúdenie zhody prijatých bezpečnostných opatrení s požiadavkami podľa tohto zákona a osobitných predpisov, ktoré sa vzťahujú na bezpečnosť sietí a informačných systémov prevádzkovateľa základnej služby pre jednotlivé siete a informačné systémy základnej služby a pre prostriedky, ktoré podporujú základné služby. Tou vopred definovanou špecifikáciou a teda kritériami auditu kybernetickej bezpečnosti sú ustanovenia zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti2, resp. vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení. Do kritérií auditu kybernetickej bezpečnosti sú v súlade s § 19 ods. 1 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti[2] zahrnuté aj sektorové bezpečnostné opatrenia, ak sú prijaté.

Proces auditu je možné zobraziť graficky. V schéme nie sú zachytené prípravné fázy auditu, napríklad stanovenie rozsahu auditu, príprava auditného programu atď. Schéma slúži len na znázornenie základných princípov auditu.



Obr. 6 Proces auditu kybernetickej bezpečnosti
(Zdroj: Vlastné spracovanie)

V zmysle platného Štandardu na výkon auditu kybernetickej bezpečnosti podľa požiadaviek zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov[26], ktorý vydal Národný bezpečnostný úrad a ktorý je záväz-

[26] Štandard na výkon auditu kybernetickej bezpečnosti v zmysle požiadaviek zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

ný pre všetkých certifikovaných audítorov kybernetickej bezpečnosti, je jednou zo všeobecných zásad auditu kybernetickej bezpečnosti prístup, založený na dôkazoch. Napriek tomu, dôkazy získavané v audite nie je možné účelom ich použitia porovnávať s potenciálnymi digitálnymi dôkazmi v kontexte digitálnej forenznej analýzy, alebo znaleckej činnosti. Účelom zberu auditných dôkazov je použiť racionálne metódy, ktorých cieľom je v systematickom procese auditovania dosiahnuť spoľahlivé a reprodukovateľné závery auditu.

V audite kybernetickej bezpečnosti je audítor povinný riadiť sa zásadou relevantnosti. Audítor musí vedieť preukázať, že získané dôkazy sú relevantné pre audit – t. j. že obsahujú informácie, ktoré majú význam pre posúdenie a že existuje opodstatnený dôvod, prečo boli získané (Relevantnosť je vlastnosť dôkazného prostriedku, ak má tento slúžiť na preukázanie alebo vyvrátenie časti konkrétnej informácie).

Všetky postupy, používané pri manipulácii s auditnými dôkazmi, by mali byť opakovateľné (Opakovateľnosť je vlastnosť procesu, vykonaného s cieľom získať rovnaké výsledky testov v rovnakom testovacom prostredí – t. j. rovnaký počítač, pevný disk, režim prevádzky atď.). Výsledky postupov by mali byť zároveň aj reprodukovateľné (Reprodukovateľnosť je vlastnosť procesu v snahe získať rovnaké výsledky testov v inom testovacom prostredí – t. j. iný počítač, pevný disk, operátor atď.).

Na rozdiel od digitálnej forenznej analýzy, primárnym cieľom auditu nie je identifikácia, zber, získavanie a uchovanie digitálnych stôp z ich pôvodných zdrojov, ale získanie objektívnych informácií, ktoré majú argumentačne podporiť zistenia auditu. Auditné dôkazy sa majú vyhodnocovať voči stanoveným kritériám auditu, s cieľom objektívne určiť zistenia auditu.

7. Získavanie auditných dôkazov

Ako dôkaz auditu by sa mali akceptovať iba také informácie, ktoré sa dajú overiť. Ak použiteľná miera overenia nie je dostatočná, audítor má použiť vlastný profesijný úsudok. Ak nie je možné zabezpečiť iný hmotný dôkaz, ako dôkaz sa použije zápisnica z auditného rozhovoru. Overením v tomto prípade bude potvrdenie člena auditného tímu, ktorý dosvedčí správnosť alebo pravdivosť auditného zistenia.

Zaznamenať sa má každý dôkaz auditu, ktorý vedie k zisteniu. Ak sa v priebehu získavania objektívnych dôkazov vyskytnú akékoľvek nové alebo zmenené skutočnosti, riziká alebo príležitosti (t. j. nové zistenia), je potrebné aj pre tieto posúdiť, aký majú vplyv na súlad, alebo nesúlad.

Metódy získavania informácií zahŕňajú najmä:
– rozhovory,
– pozorovania,
– dotazníky,
– preskúmania zdokumentovaných informácií.

Získavanie informácií pri audite sa uskutočňuje výhradne bez zásahu audítora do auditovaného informačného systému. Požadované informácie je povinný dodať zodpovedný zamestnanec, alebo kontraktor auditovanej organizácie. Táto prax taktiež predstavuje zásadný rozdiel oproti digitálnej forenznej analýze, resp. znaleckom úkone, keďže najmä v trestných konaniach nie je možné predpokladať súčinnosť, ba dokonca niekedy by mohlo byť jej vyžadovanie kontraproduktívne a viesť k znehodnoteniu potenciálnych dôkazov, neopomínajúc aj inštitúty ako odopretie výpovede alebo zákaz výsluchu.

Činnosti priamo ovplyvňujúce funkčnosť auditovaného informačného systému, ako napríklad výkon penetračných testov, výkonnostných testov a podobne, je pri audite zakázané vykonávať. Audítor by mal v rámci auditu vykonávať iba úkony, ktoré nepovedú k znehodnoteniu dôkazov či už jeho úmyselným alebo nedbanlivostným konaním. Napríklad by nemal pristupovať k takým zariadeniam, na obsluhu ktorých nemá potrebné spôsobilosti a nie je pripravený využiť spoľahlivé a overené postupy.

Obr. 7 Vzťah kvantity a kvality auditných dôkazov (Zdroj: Vlastné spracovanie)

Audit sa vykonáva počas stanoveného časového intervalu a s obmedzenými zdrojmi, teda auditný dôkaz sa môže zakladať iba na vybraných vzorkách dostupných informácií, nie na posúdení úplného súboru všet-

kých dostupných informácií. Dôveryhodnosť záverov auditu je úzko spojená s použitím primeraného vzorkovania.

Výkon auditných činností pomocou vzorkovania má za cieľ získať a overiť použiteľné informácie, týkajúce sa cieľov, predmetu a kritérií auditu, vrátane informácií, súvisiacich s rozhraním medzi funkciami, činnosťami a procesmi.

Vzorkovanie pri audite sa vykonáva najmä vtedy, ak nie je praktické alebo efektívne preverenie všetkých dostupných informácií v priebehu auditu, napríklad ak sú záznamy príliš početné alebo rozptýlené na to, aby bolo možné posúdiť každú položku v základnom súbore. Vzorkovanie veľkého súboru je proces výberu menej ako 100 % položiek z celkového dostupného dátového súboru (základného súboru) na získanie a vyhodnotenie dôkazov o nejakej vlastnosti základného súboru s cieľom formulácie záverov, týkajúcich sa základného súboru. Kvalita auditných dôkazov nie je v priamej úmere ku ich kvalite.

Získanie väčšieho množstva menej kvalitných auditných dôkazov nemusí nevyhnutne kompenzovať nedostatok kvalitných auditných dôkazov. Preto je výslovne na rozhodnutí vedúceho audítora, o získanie akých auditných dôkazov sa bude auditný tím usilovať s ohľadom na cieľ auditu.

8. Chyby v auditoch a znaleckých posudkoch

Chyby znaleckého posudku môžu byť najmä formálneho charakteru, napríklad, ak znalecký posudok neobsahuje nálezovú časť, zošívaciu šnúru, alebo nie je opatrený znaleckou pečiatkou. Formálne chybný je aj znalecký posudok, vyhotovený znalcom, ktorý nebol oprávnený na to, aby v danom odvetví vykonával znalecké úkony[27]. Vzhľadom na ustanovenie § 29 ods. 3 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti[2] možno rovnako za formálne chybnú možné považovať záverečnú správu auditu, ktorá nebola podpísaná certifikovaným audítorom.

Procesné vady znaleckého posudku sú také nedostatky, ako je zaujatosť znalca, vyhotovenie znaleckého posudku inou osobou, alebo vypracovanie znaleckého posudku na základe podkladov, ktoré boli získané inak, ako spôsobom prípustným podľa zákona. Podobne vnímanou chybou auditu kybernetickej bezpečnosti by bolo vypracovanie záverečnej správy audítorom, ktorý nie je voči objektu posúdenia nestranný (napr. v minulosti sa podieľal na vývoji, implementácii alebo prevádzke posudzovaných informačných systémov a procesov prevádzkovateľa).

[27] KŘÍSTEK, Lukáš. *Znalectví.* Praha: Wolters Kluwer, 2013, s. 223. ISBN 978-80-7478-042-4.

Metodické nedostatky môžu spočívať v skutočnosti, že znalecký posudok (alebo audit) je nedostatočne odôvodnený alebo trpí vnútornými rozpormi. Prípadne, ak znalec (alebo audítor) nevyužije všetky podklady, ktoré mu boli poskytnuté, pričom sa so zvyškom týchto údajov žiadnym spôsobom nevysporiada.[28]

Ak vzniknú pochybnosti o správnosti znaleckého posudku, alebo ak je znalecký posudok nejasný alebo neúplný, § 146 zákona č. 301/2005 Z. z. Trestný poriadok[8] umožňuje požiadať znalca o vysvetlenie alebo doplnenie posudku. Ak ani toto nevedie k odstráneniu pochybností alebo nejasností znaleckého posudku alebo k úplnosti znaleckého posudku, je možné pribrať iného znalca.

Inštitút pribratia iného audítora nie je explicitne uplatnený pri audite kybernetickej bezpečnosti. Avšak tu je kontrolný mechanizmus implementovaný prostredníctvom ustanovenia o kontrole podľa § 28 zákona č. 69/2018 Z. z. a zároveň ustanovenia o nariadenom audite podľa § 29 ods. 6 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti[2]. Národný bezpečnostný úrad môže prostredníctvom certifikovaného audítora kedykoľvek vykonať audit kybernetickej bezpečnosti u prevádzkovateľa základnej služby, alebo požiadať certifikovaného audítora kybernetickej bezpečnosti, aby vykonal takýto audit u povinnej osoby, s cieľom potvrdiť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti.[2] Pri výkone kontroly nad dodržiavaním ustanovení zákona a jeho vykonávacích predpisov postupuje Národný bezpečnostný úrad ako pri výkone kontroly v štátnej správe, podľa osobitného predpisu, ktorým je zákon č. 10/1996 Z. z. o kontrole v štátnej správe v znení neskorších predpisov.[29]

9. Diskusná časť a zistenia

Táto analýza sa nevenuje procesným otázkam dokazovania, ktoré sú predmetom iných analýz v samostatných právnych vedách. Tiež problematika vytvárania dôkazových kópií digitálnych stôp, ochrany integrity potenciálnych dôkazov, vytvárania záznamov reťazca starostlivosti (ang.: „Chain of Custody Records“), alebo uchovávania volatilných[30] stôp je predmetom podrobnejších metodík a štandardov.

---

[28] BRADÁČ, A. – KLEDUS, M. – KREJČÍŘ, P. a kol. *Soudní znalectví.* Brno : Akademické nakladatelství CERM, s.r.o., 2010, s. 104. ISBN 978-80-7204-704-8.

[29] Zákon č. 10/1996 Z. z. o kontrole v štátnej správe v znení neskorších predpisov.

[30] (z ang. „volatility“) stopy, ktoré sú obzvlášť náchylné na zmenu stavu systému alebo môžu byť ľahko pozmenené; napr. na základe straty napájania alebo prechodu cez magnetické pole a pod.

V nasledujúcom závere ide o pokus zhrnutia porovnateľných, resp. odlišných charakteristík znaleckých úkonov a auditov kybernetickej bezpečnosti, oboje ako možných dôkazných prostriedkov. Odlišnosti nie sú formulované ako konflikty, ale ako paradoxy, keďže vo väčšine identifikovaných odlišností nejde o právny či odborný rozpor, len o odlišnú interpretáciu rovnakého pojmu alebo rovnakého princípu.

V znaleckej činnosti je cieľom získať a uchovať všetky identifikované digitálne stopy, ktoré môžu byť použité v dôkaznom konaní. Dôkazom sa stopa stane, keď súd, vykonávajúci dokazovanie, rozhodne o prípustnosti dôkazov predložených v dôkaznom konaní.

Od audítora sa vyžaduje, aby získali dostatočné a relevantné informácie, ktoré poskytnú primeraný základ pre dôkaz vyjadreného odborného názoru vo vzťahu k cieľom auditu. Za dôkaz sa vyhlasuje informácia, ktorá je de facto iba stopou. Dôkazom sa získaná informácia stáva jej uvedením v záverečnej správe auditu.

V znaleckej činnosti je možný tak zber digitálnych stôp aj získavanie digitálnych stôp. To znamená, že v znalectve je bežným prístupom zhromažďovanie fyzických položiek, ktoré môžu obsahovať potenciálne digitálne dôkazy, vrátane ich odstraňovania z pôvodného umiestnenia, a rovnako aj vytváranie dôveryhodných digitálnych kópií potenciálnych dôkazov.

Audítor kybernetickej bezpečnosti nie je oprávnený odstraňovať získané dôkazy z ich pôvodného umiestnenia a povolené je výhradne získavanie (akvizícia) dôkazov, t. j. len vytváranie dôveryhodných kópií potenciálnych dôkazov.

V znaleckej činnosti je cieľom získať a uchovať všetky identifikované digitálne stopy, ktoré môžu byť použité v dôkaznom konaní a preto nie je prípustné vzorkovanie a nutné je snažiť sa o akvizíciu všetkých identifikovateľných stôp. V znalectve je kvantita získaných stôp v priamej úmere ku kvalite dôkazného prostriedku. Získanie menšieho množstva identifikovaných stôp nutne vedie ku nižšej interpretačnej hodnote dôkazného prostriedku.

V audite kybernetickej bezpečnosti je cieľom získať dostatočné a relevantné informácie, ktoré poskytnú dôkaz odborného názoru, preto za dostatočné sa považuje aj získavanie informácií na základe vzoriek. Získanie väčšieho množstva menej kvalitných auditných dôkazov nemusí nevyhnutne kompenzovať nedostatok kvalitných auditných dôkazov.

Audit môže zahŕňať aj získanie podporných informácií, ktoré pomôžu naformulovať odporúčania na zlepšenia pre auditovanú organizáciu.

V znaleckej činnosti nie je identifikácia podporných informácií primárnym účelom znaleckého úkonu. Znalec sa musí striktne držať plat-

nej osnovy posudku a poskytnúť odpovede na položené otázky, ktoré mu boli určené v objednávke znaleckého posudku, alebo v uznesení o pribratí, či ustanovení znalca. Na druhej strane, znalec môže podľa vlastného uváženia v nálezovej časti posudku uviesť aj podporné informácie, ktoré môžu napomôcť náležitému objasneniu veci.

Audítor je podľa platnej Metodiky auditu[17] povinný uchovávať záverečnú správu a všetky získané auditné dôkazy po dobu najmenej dva roky od skončenia auditu.

Znalec je v zmysle § 17 ods. 10 zákona č. 382/2004 Z. z. o znalcoch, tlmočníkoch a prekladateľoch[1] *povinný uschovávať rovnopis písomne podaného znaleckého posudku podpísaného vlastnoručným podpisom alebo podpísaného kvalifikovaným elektronickým podpisom alebo kvalifikovanou elektronickou pečaťou a opatreného kvalifikovanou elektronickou časovou pečiatkou po dobu desiatich rokov od jeho vykonania. Rovnako sa postupuje pri samostatných, k znaleckému posudku pripojených prílohách.*

Úlohou audítora kybernetickej bezpečnosti je posúdenie súladu s požiadavkami zákona, čo je nepochybne možné považovať za právne závery, príp. závery, významné pre možný budúci právny postup správneho orgánu voči auditovanému subjektu.

Oprávnením znalca nie je riešenie právnych otázok ani hodnotenie vykonaných dôkazov.

Kritériá auditu kybernetickej bezpečnosti sú ustanovenia zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti[2], resp. vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení. Do kritérií auditu kybernetickej bezpečnosti sú zahrnuté aj sektorové bezpečnostné opatrenia, ak sú prijaté.

Pre znaleckú činnosť nie je vopred vymedzená akákoľvek špecifikácia. Znalec použije všetky svoje odborné znalosti a informácie (dostupné z najlepšej praxe) k tomu, aby odpovedal na skutkové odborné otázky, položené zadávateľom. Povinne je právnym predpisom určená len forma a osnova posudku.[22]

Chyby záverečnej správy auditu je možné identifikovať iba následným auditom, alebo kontrolou zo strany Národného bezpečnostného úradu. Kontrolný mechanizmus je implementovaný prostredníctvom ustanovenia o kontrole podľa § 28 a zároveň ustanovenia o nariadenom audite podľa § 29 ods. 6 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti.[2] Ak by sa v rámci následného auditu preukázalo, že audítor v predchádzajúcom audite vychádzal z rovnakého a nezmeneného, avšak nesprávne vyhodnoteného dôkazu, alebo ak následný audit usku-

toční odlišné závery, pretože audítor v predchádzajúcom audite v rámci vzorkovania vychádzal z nedostatočných dôkazov, je možné zistenie z predchádzajúceho auditu vyhodnotiť ako chybné. To síce nie je trestným činom, avšak pri opakovanom chybnom konaní alebo opomenutí konania na strane audítora, ktoré by bolo vyhodnotené ako porušujúce platné pravidlá a požiadavky, je certifikačný orgán povinný z vlastnej činnosti alebo na základe podnetu Národného bezpečnostného úradu pozastaviť platnosť vydaného certifikátu audítora.

Nejasný alebo neúplný znalecký posudok vedie k možnosti požiadať znalca o vysvetlenie alebo doplnenie posudku v zmysle § 146 zákona č. 301/2005 Z. z. Trestný poriadok.[8] V prípade, že nedôjde k odstráneniu pochybností alebo nejasností znaleckého posudku, je možné pribrať iného znalca. Ak znalec pred súdom, prokurátorom alebo policajtom v trestnom konaní, alebo pred súdom v občianskom súdnom konaní, alebo v exekučnom konaní, alebo v konaní pred orgánom verejnej správy, alebo pred rozhodcovským súdom, uvedie nepravdu o okolnosti, ktorá má podstatný význam pre rozhodnutie, alebo takú okolnosť zamlčí, alebo pri podávaní znaleckého posudku na podklade zmluvy inému spôsobí škodu tým, že uvedie nepravdu o okolnosti, ktorá má podstatný význam pre osobu, ktorej sa znalecký posudok týka, alebo má podstatný význam pre rozhodnutie, ktorého je znalecký posudok podkladom, alebo ak takú okolnosť zamlčí, dopustí sa trestného činu nepravdivého znaleckého posudku, tlmočníckeho úkonu a prekladateľského úkonu podľa § 347 zákona č. 300/2005 (Trestný zákon).[31]

Úlohy audítora kybernetickej bezpečnosti sú stanovené v štandarde *Metodika auditu kybernetickej bezpečnosti*[17], ktorý vydal Národný bezpečnostný úrad a ktorý je záväzný pre všetkých certifikovaných audítorov kybernetickej bezpečnosti.

Úlohy, ktoré má riešiť znalec, sa mu určia vopred, spravidla v objednávke znaleckého posudku, alebo v uznesení o pribratí či ustanovení znalca, a to formou otázok.

V audite sú metódami akvizície stôp a potenciálnych dôkazov výhradne auditné rozhovory, pozorovania, auditné dotazníky a pasívne preskúmanie zdokumentovaných informácií. Audítor nesmie použiť metódy, ktoré by akokoľvek ovplyvnili činnosť auditovaného informačného systému. Audítor by mal v rámci auditu vykonáva iba úkony, ktoré nepovedú k znehodnoteniu dôkazov.

V znaleckom úkone sú povolené akékoľvek metódy akvizície stôp a potenciálnych dôkazov, ak nie je možné využiť iné slabiny v systéme, ktoré by uľahčili získanie digitálnych stôp. Takými metódami sú naprí-

[31] Zákon č. 300/2005 (Trestný zákon).

klad výkon penetračných testov, vrátane invazívnych metód, kryptoanalytických útokov alebo metód za použitia útoku hrubou silou (z angl.: „brute-force attack“). Fakt, že tieto úkony môžu viesť k znehodnoteniu bitových kópií pôvodných digitálnych stôp, nie je prekážkou, ak si znalec pred použitím metód útoku hrubou silou vytvorí redundantné bitové kópie pôvodných digitálnych stôp.

Zhodne v znaleckom úkone aj v záverečnej správe auditu musí byť uvedený postup použitý pri vyhodnocovaní potenciálnych dôkazov.

Znalec uvedie opis predmetu znaleckého skúmania a skutočností, na ktoré pri úkone znaleckej činnosti prihliadal, uvedie postup, na základe ktorého sa dopracoval k odpovediam na otázky položené zadávateľom a k splneniu ním uložených úloh.

Audítor určí metódy a postupy auditu a zvolí vhodné nástroje, potrebné pre audit vopred, ešte v rámci procesu stanovenia rozsahu trvania auditu.

Pre znalecký úkon aj pre záverečnú správu auditu musí byť zabezpečená ich dodatočná preskúmateľnosť.

Zákon o znalcoch[1] v ustanovení § 17 ods. 5 stanovuje, že celková skladba znaleckého posudku musí umožniť preskúmať jeho obsah a overiť odôvodnenosť postupov.

Metodika auditu[17] v čl. 1.4.8 stanovuje, že všetky postupy používané pri manipulácii s auditnými dôkazmi by mali byť opakovateľné a zároveň reprodukovateľné.

Podľa väčšiny metodík, či už sa týkajú znaleckých úkonov alebo získavania auditných dôkazov, sa výkon týchto činností riadi tromi základnými princípmi:

- relevancia – audítor, či znalec by mali byť schopní preukázať, že získané informácie sú relevantné pre vyvodenie záverov, t. j. že majú význam pre ďalšiu analýzu a že existuje dobrý dôvod, prečo boli získané,
- spoľahlivosť – audítor, či znalec by mali byť schopní preukázať, že všetky procesy použité pri manipulácii s potenciálnymi digitálnymi dôkazmi sú kontrolovateľné a opakovateľné, s neustálou snahou o zachovanie integrity a dôveryhodnosti získaných informácií,
- dostatočnosť – audítor, či znalec by sa mali ubezpečiť, že bol získaný dostatok údajov, aby bolo možné vykonať analýzu a vyvodiť z nej závery.

Pre obe analyzované odborné činnosti spojené s dokazovaním v kybernetickej bezpečnosti platí univerzálna zásada a to, že obe roly majú byť zásadne nezávislé od objektu posudzovania a vždy majú konať spôsobom, ktorý vylúči tendenčnosť a konflikt záujmov. Tak

audítor kybernetickej bezpečnosti, ako aj znalec, zapísaný v príslušnom znaleckom odvetví, majú vykonávať dokazovanie poctivo, zodpovedne, objektívnym a nezaujatým spôsobom.

Záver

Výkon znaleckej činnosti podľa zákona č. 382/2004 Z. z. o znalcoch, tlmočníkoch a prekladateľoch a o zmene a doplnení niektorých zákonov[1] a výkon auditu kybernetickej bezpečnosti podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov[2] majú niekoľko porovnateľných, ale najmä niekoľko zásadne odlišných charakteristík procesov dokazovania.

Zhodné charakteristiky sa dajú stručne zhrnúť nasledovne:

- Rovnako v znaleckom úkone ako aj v záverečnej správe auditu musí byť uvedený postup použitý pri vyhodnocovaní potenciálnych dôkazov.
- Znalecký úkon aj záverečná správa auditu musia umožňovať dodatočnú preskúmateľnosť.
- Základné, najmä etické princípy znaleckých úkonov ako aj auditu kybernetickej bezpečnosti sú totožné: nestrannosť, nezávislosť, zodpovednosť, objektivita.

Oproti tomu existuje viac charakteristík, ktoré sú v niektorých prípadoch rozdielne až do tej miery, že spôsobujú terminologické a interpretačné problémy:

- V znalectve je bežným prístupom zhromažďovanie fyzických položiek, ktoré môžu obsahovať potenciálne dôkazy. Pri výkone auditu kybernetickej bezpečnosti je povolené len vytváranie dôveryhodných kópií potenciálnych dôkazov.
- V znaleckej činnosti je cieľom získať všetky použiteľné informácie. V audite kybernetickej bezpečnosti je dostatočné aj získavanie informácií na základe vzoriek.
- Súčasťou záverečnej správy auditu typicky bývajú aj odporúčania nad rámec kontrolného zoznamu. Znalec poskytuje odpovede primárne na otázky, ktoré mu boli položené v zadaní.
- Záverečná správa auditu musí byť uchovaná po dobu dvoch rokov. Rovnopis znaleckého posudku musí byť uchovaný po dobu desiatich rokov.
- Znalec nie je oprávnený riešiť právne otázky ani hodnotiť vykonané dôkazy. Úlohou audítora kybernetickej bezpečnosti je naopak práve posúdenie súladu s požiadavkami zákona.

– Obsah auditu kybernetickej bezpečnosti je určený všeobecne záväznými právnymi predpismi. Znalecký úkon nemá vopred vymedzenú špecifikáciu výsledného obsahu.
– Chyby záverečnej správy auditu je možné identifikovať následným auditom, alebo kontrolou NBÚ, pričom sankciou môže byť pozastavenie platnosti vydaného certifikátu audítora. Chyby znaleckého posudku môže odhaliť pribratie iného znalca a vypracovanie nového posudku, pričom však úmyselne chybný posudok môže napĺňať skutkovú podstatu trestného činu.
– Úlohy audítora kybernetickej bezpečnosti sú stanovené v záväznej metodike. Znalcovi sa úlohy určia vždy ad-hoc, formou otázok.
– Audítor nesmie použiť metódy, ktoré by viedli k znehodnoteniu dôkazov, alebo ktoré by ovplyvnili auditované prostredie. Znalec môže použiť aj invazívne metódy, kryptoanalytické útoky alebo metódy za použitia útoku hrubou silou nad kópiami pôvodných digitálnych stôp zo skúmaného prostredia.

Dôkazy sú získané, agregované informácie o stopách, ktoré môžu byť použité na podporu tvrdení alebo aj na ich vyvrátenie. Každá informácia, ktorú je možné považovať za relevantnú pre konkrétny problém, je zároveň stopou a potenciálnym dôkazom súčasne. V auditných procesoch má už samotný výraz „dôkaz“ zásadne odlišný význam, ako v znaleckých činnostiach. Za dôkaz je v audite pomenovaná informácia, ktorá je v čase jej získania ešte len stopou, tzn. potenciálnym dôkazom, preto sa dá tvrdiť, že pri audite sa termín „dôkaz“ používa nekorešpondujúcim spôsobom.

Podľa ústavného súdu imanentným znakom právneho štátu patrí neodmysliteľne aj princíp právnej istoty, ktorého súčasťou je tiež požiadavka, aby sa na určitú právne relevantnú otázku pri opakovaní v rovnakých podmienkach dala rovnaká odpoveď[32]. Inými slovami: obdobné situácie musia byť rovnakým spôsobom právne posudzované. V znaleckej činnosti súvisiacej s akvizíciou digitálnych stôp a ich použití v dôkaznom konaní ako aj v procesoch dokazovania pri výkone auditu kybernetickej bezpečnosti sa jedná o obdobné situácie.

Vyššie v tejto práce bolo dôvodené, že pre otázky súvisiace s akvizíciou digitálnych stôp, dokazovania a vykonávania potenciálnych dôkazov pomocou dôkazných prostriedkov v kontexte kybernetického priestoru sú vecne príslušnými orgánmi štátnej správy Ministerstvo spravodlivosti Slovenskej republiky a Národný bezpečnostný úrad.

[32] Napr. I. ÚS 87/93, PL. ÚS 16/95 a II. ÚS 80/99.

V Slovenskej republike v súčasnosti neexistuje všeobecne záväzný právny predpis, ani technická norma, ktoré poskytovali usmernenia pre konkrétne činnosti pri nakladaní s digitálnymi dôkazmi a uchovávaním informácií, ktoré môžu mať potenciálnu dôkaznú hodnotu. Bolo by efektívne, ak by príslušné orgány verejnej moci spracovali právne záväzné ukotvenie postupov pre identifikáciu, zber, získavanie a uchovávanie digitálnych dôkazov. Taktiež by bolo účelné navrhnúť také zmeny a doplnenia ustanovení príslušných právnych predpisov, ktoré by zjednotili terminológiu týkajúcu sa vykonávania potenciálnych dôkazov pomocou dôkazných prostriedkov v kontexte kybernetického priestoru.

Použitá literatúra

1. Zákon č. 382/2004 Z. z. o znalcoch, tlmočníkoch a prekladateľoch a o zmene a doplnení niektorých zákonov.
2. Zákon č. 69/2018 Z. z. *o kybernetickej bezpečnosti* a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
3. Vyhláška Národného bezpečnostného úradu č. 493/2022 Z. z. o audite kybernetickej bezpečnosti.
4. ISO/IEC 27037:2012 *Informačné technológie – Bezpečnostné metódy – Návod na identifikáciu, zber, získavanie a uchovávanie digitálnych dôkazov.*
5. KAČALA, J. – PISÁRČIKOVÁ, M. – POVAŽAJ, M. a kol. *Krátky slovník slovenského jazyka 4. dopl. a upr. vyd.* Bratislava : Veda 2003. 985 s. ISBN 80-224-0750-X.
6. STRAUS, Jiří – VAVERA, František. *Slovník kriminalistických pojmů a osobností*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2010. ISBN 978-80-7380-258-5.
7. SHOWN MILLS Elizabeth. *Is It Evidence or ‚Just a Clue'? blog post, QuickTips: The Blog @ Evidence Explained*. 15 September 2018. [online], URL: https://www.evidenceexplained.com/index.php/quicktips/is-it-evidence-or-just-a-clue
8. Zákon č. 301/2005 Z. z. *Trestný poriadok* v znení neskorších predpisov.
9. Zákon č. 160/2015 Z. z. *Civilný sporový poriadok* v znení neskorších predpisov
10. JELÍNEK, Jiří. *Trestní zákoník a trestní řád: s poznámkami a judikaturou.* 7. aktualizované vydání podle stavu k 1.10.2017. Praha: Leges, 2017
11. ŠIMOVČEK, I. *Prípustnosť dôkazov v trestnom konaní. In Teoretické a praktické problémy dokazovania*. Eurokódex, 2008, s. 255. EAN 9788089363223.

12. MOLITORIS, Peter. *Vzťah medzi zákonnosťou a prípustnosťou dôkazov vo veciach správneho trestania.* STUDIA IURIDICA Cassoviensia, ročník 6.2018, číslo 1, 33. ISSN 1339-3995.
13. POLČÁK, Radim – PÚRY, František – HARAŠTA, Jakub a kol. *Elektronické důkazy v trestním řízení.* 1. vyd. Brno : Masarykova univerzita, Právnická fakulta, 2015. 253 s. Spisy Právnické fakulty Masarykovy univerzity, řada teoretická, Edice Scientia č. 542. ISBN 978-80-210-8073-7.
14. BOULDING, Kenneth. *Notes on the Information Concept.* Exploration. Toronto. 6: 103–112. CP IV, (1955) str. 21–32.
15. HENRY, Nicholas L. *Knowledge Management: A New Concern for Public Administration*. Public Administration Review, vol. 34, no. 3, 1974, str. 189–96. JSTOR 974902. https://doi.org/10.2307/974902.
16. FRICKÉ, Martin. *Data-Information-Knowledge-Wisdom (DIKW) Pyramid, Framework, Continuum*. V Encyclopedia of Big Data, 1–4. Cham: Springer International Publishing, 2018. https://doi.org/10.1007/978-3-319-32001-4_331-1. ISBN: 978-3-319-32001-4.
17. ALLEN, Greenwood. *Hierarchy of Knowledge – from Data to Wisdom.* (2017). International Journal of Current Research in Multidisciplinary (IJCRM) ISSN: 2456-0979.
18. Vyhláška Ministerstva spravodlivosti SR č. 228/2018 Z. z. ktorou sa vykonáva zákon č. 382/2004 Z. z. o znalcoch, tlmočníkoch a prekladateľoch a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
19. Zákon č. 71/1967 Zb. o správnom konaní (správny poriadok) v znení neskorších predpisov.
20. Zákon č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov.
21. STN EN ISO 19011: 2019 *Návod na auditovanie systémov manažérstva* (ISO 19011: 2018).
22. *Štandard na výkon auditu kybernetickej bezpečnosti* v zmysle požiadaviek zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
23. KŘÍSTEK, Lukáš. *Znalectví*. Praha: Wolters Kluwer, 2013, s. 223. ISBN 978-80-7478-042-4.
24. BRADÁČ, A. – KLEDUS, M. – KREJČÍŘ, P. a kol. *Soudní znalectví*. Brno : Akademické nakladatelství CERM, s.r.o., 2010, s. 104. ISBN 978-80-7204-704-8.
25. Zákon č. 10/1996 Z. z. *o kontrole v štátnej správe* v znení neskorších predpisov
26. Zákon č. 300/2005 (Trestný zákon).