Kompetenčné
a certifikačné
centrum
kybernetickej
bezpečnosti

# OVEROVANIE ÚROVNE KYBERNETICKEJ BEZPEČNOSTI

FEI TUKE, 7.12.2022

Ivan Makatura

# KOMPETENČNÉ A CERTIFIKAČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI

- Pôsobnosť **Národného koordinačného centra** v zmysle Nariadenia EÚ č. 2021/887 o Európskej sieti centier odvetvových, technologických a výskumných kompetencií
- **Certifikácia:**
  - audítorov a manažérov kybernetickej bezpečnosti
  - systémov manažérstva
  - produktov v kybernetickej bezpečnosti podľa Nariadenia EÚ č. 2019/881
- **Vzdelávanie dospelých** v kybernetickej bezpečnosti
- Organizácia kampaní na zvyšovanie povedomia v kybernetickej bezpečnosti
- Publikačná činnosť
- **Audit kybernetickej bezpečnosti** podľa zákona č. 69/2018 Z. z.
- Konzultačné služby v oblasti kybernetickej bezpečnosti, utajovaných skutočností a dôveryhodných služieb
- Znalecká a expertízna činnosť podľa zákona č. 382/2004 Z. z. o znalcoch

# OBSAH PREDNÁŠKY

- typické mechanizmy a metódy overovania úrovne kybernetickej bezpečnosti
- analýza hrozieb a rizík
- základy posudzovania, testovania, auditu a certifikácie kybernetickej bezpečnosti
- posudzovanie zhody v kybernetickej bezpečnosti
- základ metodiky auditu kybernetickej bezpečnosti
- znalectvo v elektrotechnike a znalecké odvetvia relevantné pre kybernetickú bezpečnosť
- spôsob výkonu znaleckej činnosti
- kybernetická bezpečnosť v civilnom sporovom konaní a v trestnom konaní
- základy akvizície digitálnych stôp
- základy forenznej analýzy

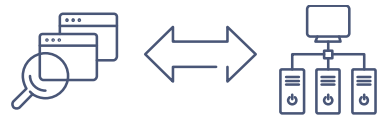
# OVEROVANIE ÚROVNE KYBERNETICKEJ BEZPEČNOSTI

OVEROVANIE ÚROVNE KYBERNETICKEJ BEZPEČNOSTI

# METÓDY OVEROVANIA ÚROVNE BEZPEČNOSTI

- Overované entity a prvky sú v procese overovania úrovne bezpečnosti všeobecne nazývané ako „**objekty posúdenia**“ (z angl. „assessment objects“)
- Štyri základné prístupy ako sa môže subjekt uistiť o požadovanej úrovni KB:

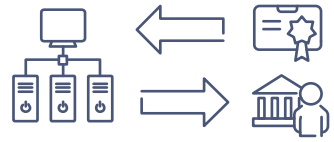
1. **Posúdenie** - Dokazovanie, že sa splnili určené požiadavky týkajúce sa objektu posudzovania



2. **Testovanie** - Proces, v ktorom je jeden alebo viac objektov posudzovania vystavených podľa opakovateľného postupu určitým podmienkam, s cieľom porovnať ich aktuálne a očakávané charakteristiky

3. **Audit** - 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

4. **Certifikácia** (Posudzovanie zhody) - Atestácia nezávislým akreditovaným orgánom posudzovania zhody, týkajúca sa charakteristík objektu posudzovania

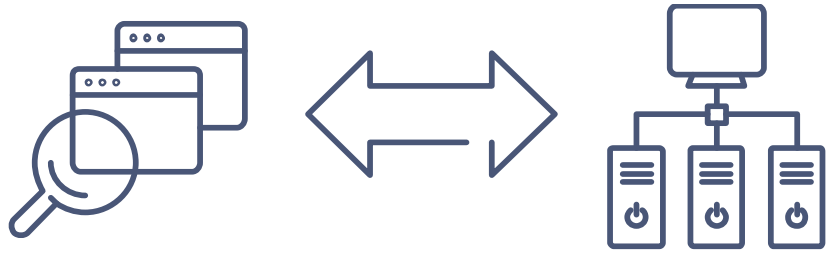


# POSUDZOVANIE BEZPEČNOSTI

Dokazovanie, že sa splnili určené požiadavky týkajúce sa objektu posudzovania

**Typické metódy:**

- Analýza rizík
- Rozdielová analýza
- Analýza súladu
- Analýza funkčných dopadov (BIA)
- Porovnávanie v rámci odvetvia (benchmarking)
- Prieskum



**Primárny účel:**

- Poskytnúť ucelenú informáciu o stave KB a rizikách KB formou technickej správy
- Použiť konsolidované výstupy na sledovanie trendu (napr. KRI/KPI )

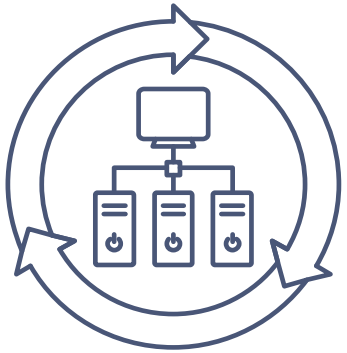
Pre posudzovanie je typické, že môže byť vykonané vlastným hodnotením

# TESTOVANIE BEZPEČNOSTI

Proces, v ktorom je jeden alebo viac objektov posudzovania vystavených podľa opakovateľného postupu určitým podmienkam, s cieľom porovnať ich aktuálne a očakávané charakteristiky

**Typické metódy:**

- Detekcia zraniteľností , scannovanie zraniteľností
- Penetračné testovanie
- Revízia softvérového kódu (code review)
- Integračné testovanie
- Výkonnostné testovanie (performance test)



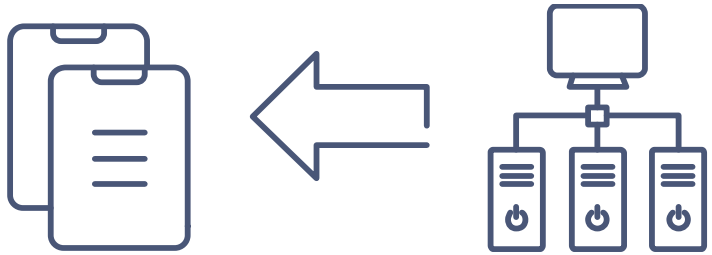
**Primárny účel:**

- Získanie informácií o charakteristikách objektov v kontexte KB

Pre testovanie je typická požiadavka na vysokú mieru zručnosti

# AUDIT BEZPEČNOSTI

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



**Typické metódy:**

- Auditné rozhovory a dotazníky
- Porovnávanie deklarovaného a skutkového stavu
- Preskúmanie zdokumentovaných informácií
- Vzorkovanie (vykonáva sa, ak nie je praktické alebo efektívne preverenie všetkých dostupných informácií v priebehu auditu)

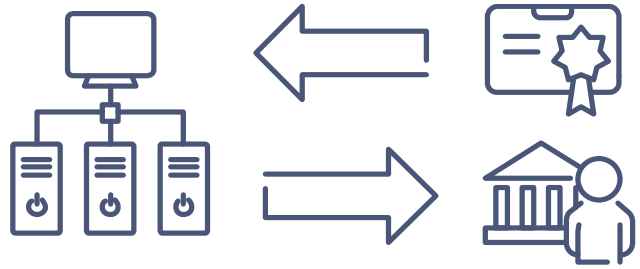
**Primárny účel:**

- Získanie informácie o nezhodách a rizikách formou konsolidovanej správy
- Iniciácia návrhov na zmenu jestvujúcich resp. Implementáciu ďalších bezpečnostných opatrení

Pre audit je typická požiadavka na nestrannosť

# CERTIFIKÁCIA BEZPEČNOSTI

Atestácia nezávislým akreditovaným orgánom posudzovania zhody, týkajúca sa charakteristík objektu posudzovania



**Typický proces:**

1. **Žiadosť** o posúdenie zhody
2. **Vyhodnotenie** (overenie, že objekt spĺňa kvalifikačné kritériá)
3. **Atestácia** (rozhodnutie o splnení kvalifikačných kritérií)
4. **Dohľad** (priebežné posudzovanie, že objekt naďalej spĺňa kritériá)

**Primárny účel:**

- Deklarácia primeranej úrovne kybernetickej bezpečnosti výrobkov, služieb a procesov
- Posilnenie transparentnosti posudzovania a dôvery v bezpečnosť výrobkov, služieb a procesov

Pre certifikáciu je typická požiadavka na akreditáciu a dohľad

# POROVNANIE METÓD OVEROVANIA ÚROVNE BEZPEČNOSTI

| Metóda | Určený nástroj | Opakovateľný postup | Formálna špecifikácia | Nestrannosť | Dôkazy | Certifikovaná osoba | Akreditácia | Dohľad |
|---|---|---|---|---|---|---|---|---|
| **Posudzovanie** | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| **Testovanie** | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ |
| **Audit** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ |
| **Certifikácia** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

# POSUDZOVANIE ZHODY V KYBERNETICKEJ BEZPEČNOSTI

OVEROVANIE ÚROVNE KYBERNETICKEJ BEZPEČNOSTI

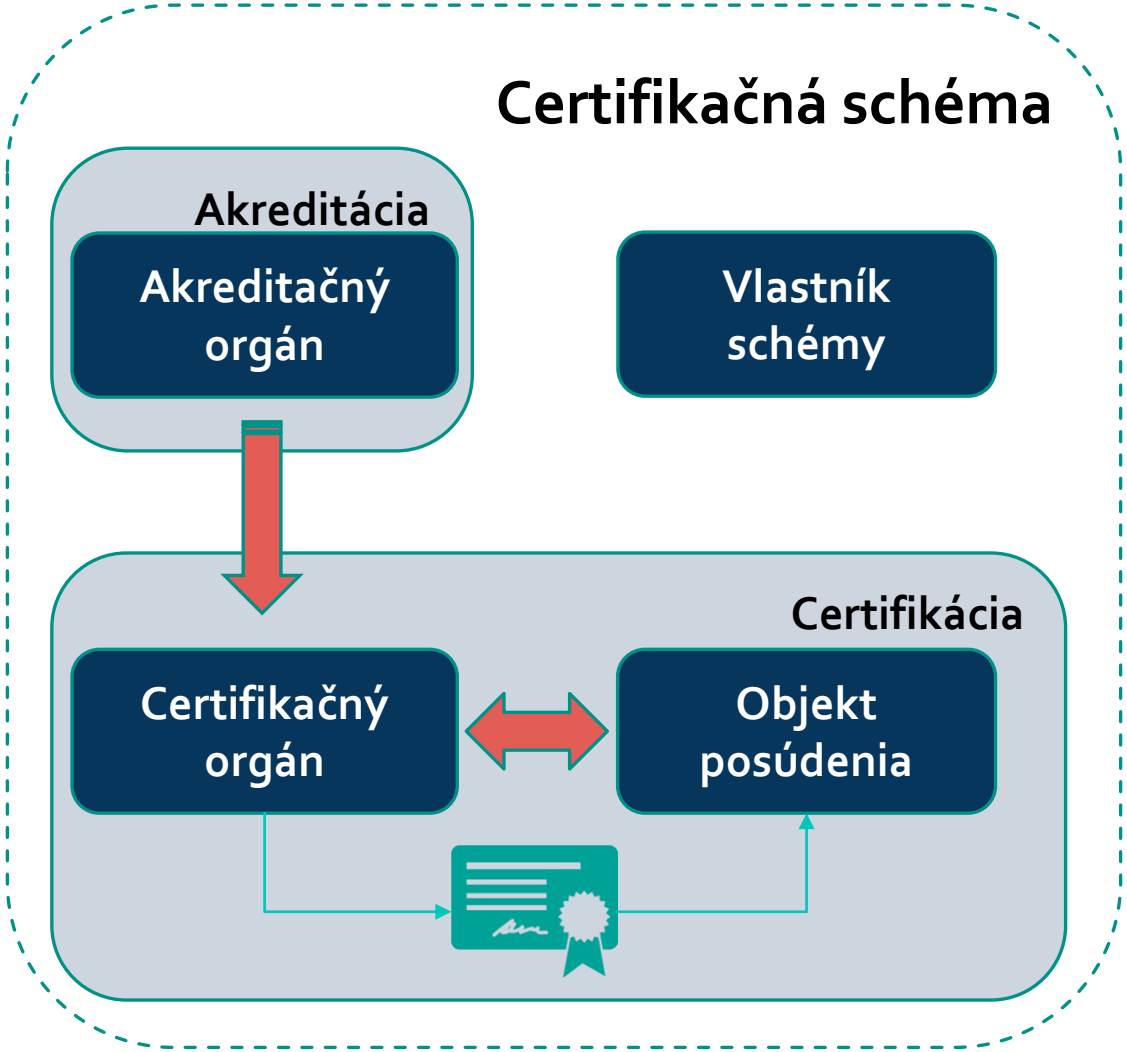
# PROCES AKREDITÁCIE PRE POSUDZOVANIE ZHODY

- **Certifikačná schéma**: systém certifikácie, ktorý sa vzťahuje na určené produkty, na ktoré sa aplikujú rovnaké určené požiadavky, osobitné pravidlá a postupy.
(ISO/IEC 17065: 2012, čl. 3.9)

- **Akreditačný orgán**: autoritatívny orgán, ktorý vykonáva akreditáciu. (V Slovenskej republike je vnútroštátnym akreditačným orgánom Slovenská národná akreditačná služba - SNAS. Postavenie SNAS a jej pôsobnosť určuje zákon č. 505/2009 Z. z. o akreditácii orgánov posudzovania zhody)
(STN EN ISO/IEC 17000: 2005, čl. 2.6)

- **Certifikačný orgán**: orgán vykonávajúci posudzovanie zhody treťou stranou podľa certifikačnej schémy
(ISO/IEC 17065: 2012, čl. 3.12)

- **Certifikácia**: atestácia treťou stranou týkajúca sa produktov, procesov, systémov alebo osôb.
(STN EN ISO/IEC 17000: 2005, čl. 5.5)



# AKREDITÁCIA PRE POSUDZOVANIE ZHODY V OBLASTI KYBERNETICKEJ BEZPEČNOSTI




## STN EN ISO/IEC 17021-1

- Posudzovanie zhody - požiadavky na orgány **vykonávajúce audit a certifikáciu systémov manažérstva**

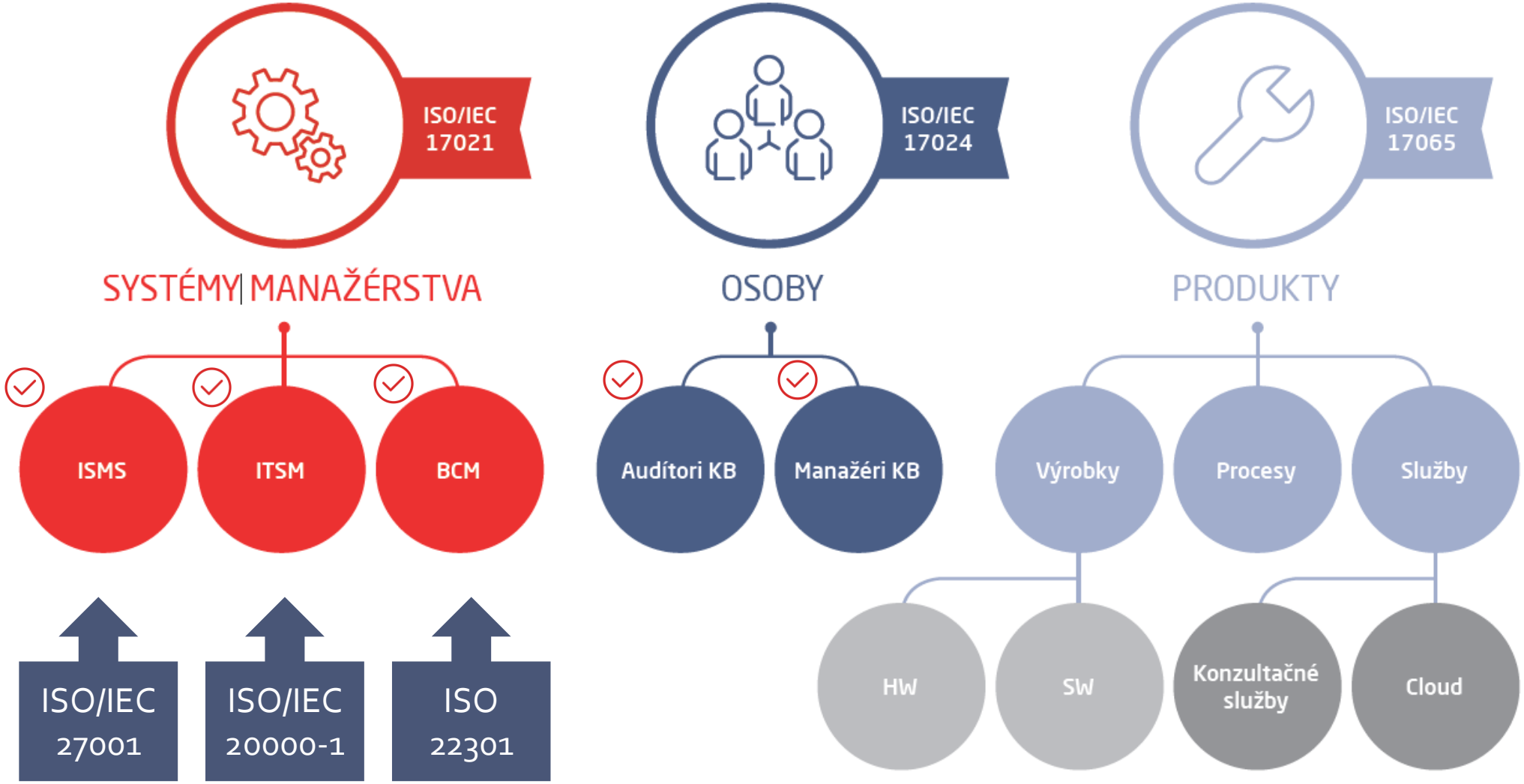
## STN EN ISO/IEC 17024

- Posudzovanie zhody - všeobecné požiadavky na orgány **vykonávajúce certifikáciu osôb**

## STN EN ISO/IEC 17065

- Posudzovanie zhody - požiadavky na orgány **vykonávajúce certifikáciu výrobkov, procesov a služieb**

# OBJEKTY POSUDZOVANIA ZHODY V OBLASTI KYBERNETICKEJ BEZPEČNOSTI



# EURÓPSKY RÁMEC CERTIFIKAČNÝCH SCHÉM

**Kandidátske schémy (draft):**

- EUCS - Certifikačná schéma pre cloudové služby
- EUCC - Certifikačná schéma pre všeobecné IKT produkty
- EU5G - Certifikačná schéma pre 5G siete


**Pripravované:**

- Certifikačná schéma pre IoT
- Certifikačné schéma pre zdravotnícke zariadenia
- Certifikačné schéma pre kognitívne systémy

# Audit kybernetickej bezpečnosti

OVEROVANIE ÚROVNE KYBERNETICKEJ BEZPEČNOSTI

# TVORBA ZISTENÍ V AUDITE KYBERNETICKEJ BEZPEČNOSTI

- Účinnosť prijatých bezpečnostných opatrení
- Plnenie požiadaviek stanovených zákonom

- Vyhláška 362/2018 Z.z. (pre ITVS / PZS)
- Vyhláška 179/2020 Z.z.
- Príslušné technické normy (ISO/IEC 27002, ISO/IEC 27018 a i.)

- Zákon č. 69/2018 Z.z. (pre ITVS / PZS)
- Zákon č. 95/2019 Z. z.

**Požiadavka**

- Bezpečnostné opatrenie podľa vyhlášky
- Formálne požiadavky v zmysle zákona

**Nezhoda**

- Chýbajúce opatrenie
- Neefektívne opatrenie
- Nesplnená požiadavka
- Neplnený bezp. cieľ
- Nedostatočná kvalita alebo rozsah dokumentácie

**Dôkaz**

- Identifikované riziko
- Identifikovaná nezhoda s požiadavkou Vyhlášky alebo Zákona
- Identifikovaná nízka účinnosť opatrenia

# Digitálna forenzná analýza z procesného pohľadu

OVEROVANIE ÚROVNE KYBERNETICKEJ BEZPEČNOSTI

# FORENZNÉ VEDY

- **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, 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 „digitálnu" analýzu

# CIELE FORENZNEJ ANALÝZY

- **Ciele forenznej analýzy**: zaručiť vykonanie špecifických činností pri zaobchádzaní s potenciálnymi dôkazmi, najmä:
  - Identifikácia (digitálnych) stôp
  - Zber, alebo získavanie stôp
  - Uchovanie stôp ako potenciálnych dôkazov

- Vyspelosť týchto činností napomôže **zachovať integritu potenciálnych dôkazov prijateľnou metodológiou pri získavaní stôp**, ktorá prispeje k ich prípustnosti v právnych a disciplinárnych konaniach
- Dobrá prax forenznej analýzy poskytuje všeobecné usmernenia pre zhromažďovanie aj iných ako digitálnych stôp, ktoré môžu byť užitočné vo fáze analýzy potenciálnych digitálnych dôkazov (fyzické stopy)

# ZAINTERESOVANÉ STRANY FORENZNEJ ANALÝZY

**Osoby typicky zodpovedné za identifikáciu, zber, získanie a uchovanie** potenciálnych (digitálnych) dôkazov:

- V pracovno-právnych vzťahoch:
  - špecialisti informačnej bezpečnosti
  - špecialisti na riešenie incidentov
  - manažéri kybernetickej bezpečnosti
  - manažéri forenzných laboratórií
  - audítori
- Vo vyšetrovaniach a súdnych sporoch:
  - forenzní technici (z angl. „Digital Evidence First Responders" - DEFR),
  - forenzní špecialisti (z angl. „Digital Evidence Specialists - DES),
  - **súdni znalci zapísaní v príslušnom odvetví a znaleckom odbore**

# ZAINTERESOVANÉ STRANY FORENZNEJ ANALÝZY

**Osoby typicky účastné na konaní** (vo všeobecnosti osoby ktoré potrebujú určiť a preukázať spoľahlivosť predložených digitálnych dôkazov):

- V pracovno-právnych vzťahoch:
  - špecialisti fraud managementu
  - HR špecialisti
  - audítori
- Vo vyšetrovaniach a súdnych sporoch:
  - orgány činné v trestnom konaní (v zmysle §10 ods. 1 TP - prokurátor a policajt)
  - súdy
  - obhajcovia, advokáti
  - strany sporu, poškodený, obvinený, obžalovaný, osoby s obhajovacími právami (zákonný zástupca, opatrovník, orgány starostlivosti o mládež, a.i.)

# Znalecká činnosť

OVEROVANIE ÚROVNE KYBERNETICKEJ BEZPEČNOSTI

# VÝKON SÚDNICTVA

**§ 2 zákona č. 757/2004 Z.z. Zákon o súdoch:**

1) Pri výkone súdnictva súdy v Slovenskej republike
   a) prejednávajú a rozhodujú spory a iné **právne veci v civilnom procese** (t.j. „**občianskoprávne veci**"),
   b) prejednávajú a rozhodujú **trestné veci podľa predpisov o trestnom konaní** (t.j. „**trestnoprávne veci**"),
   c) konajú a rozhodujú o **žalobách alebo o opravných prostriedkoch proti rozhodnutiam**, zásahom, iným opatreniam alebo nečinnosti v oblasti verejnej správy, rozhodujú o zákonnosti rozhodnutí a postupu orgánov verejnej moci a o ochrane pred nezákonným zásahom alebo opatrením orgánu verejnej moci, v prípadoch ustanovených zákonom rozhodujú vo volebných veciach, vo veciach referenda a vo veciach politických strán a hnutí, ak tak ustanoví zákon, a v ďalších veciach, ak to ustanovuje zákon (t.j.„**správne veci**"),
2) Súdy vykonávajú aj inú činnosť súvisiacu s ich právomocou, ak tak ustanoví zákon, právne záväzný akt Európskych spoločenstiev a Európskej únie alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná.

**Sústava súdov:**

Ústavný súd Slovenskej republiky,
so sídlom v Košiciach
(nepatrí do sústavy súdov SR,
je samostatným súdnym orgánom ochrany ústavnosti)

Najvyšší súd Slovenskej republiky

Krajské súdy (8)

Okresné súdy (54)

Špecializovaný trestný súd s postavením krajského súdu

# HLAVNÉ ROZDIELY V KONANIACH

## Civilné konanie

- **Každý má právo domáhať sa na súde ochrany práva, ktoré bolo ohrozené alebo porušené**
- Civilné súdne konanie je spôsobom riešenia sporov medzi dvomi (príp. i viacerými) osobami
- Súdne konanie v civilných veciach upravuje **Civilný sporový poriadok poriadok** (ďalej len „CSP"), a **Civilný mimosporový poriadok** v platnom znení
- **Strany majú v konaní rovné postavenie** spočívajúce v rovnakej miere možností uplatňovať prostriedky procesného útoku a prostriedky procesnej obrany
  - okrem prípadu, ak povaha prejedávanej veci vyžaduje zvýšenú ochranu strany sporu s cieľom vyvažovať prirodzene nerovnovážne postavenie strán sporu

## Trestné konanie

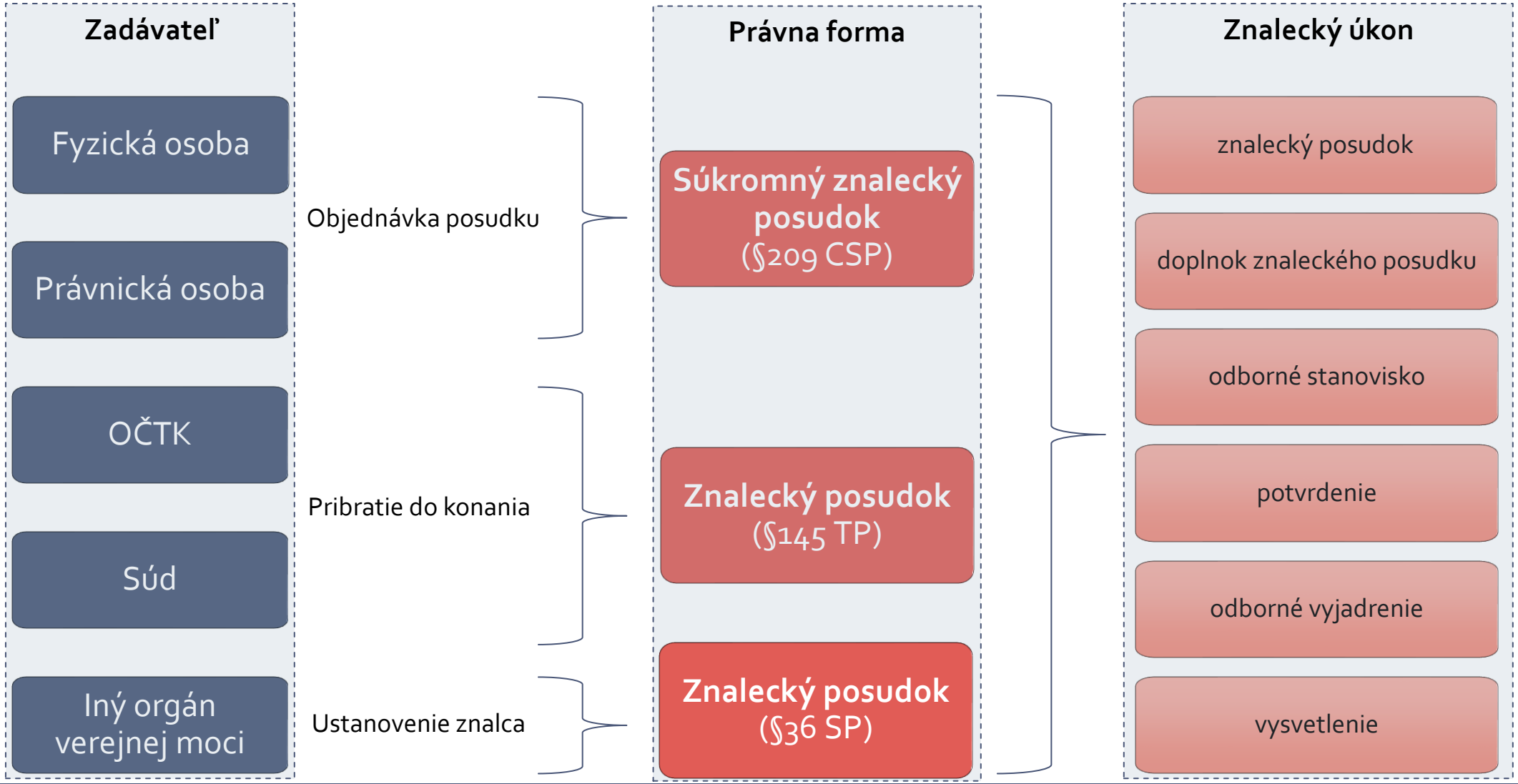
- Trestné stíhanie pred súdom je **možné len na základe návrhu alebo obžaloby podanej prokurátorom**
- V trestnom konaní pred súdom obžalobu alebo návrh zastupuje prokurátor v mene štátu
- Postup orgánov činných v trestnom konaní a súdov upravuje **Trestný poriadok** (ďalej len „TP"), v platnom znení
- V trestnom konaní pred súdom sú stranami konania:
  - ten, proti komu sa vedie trestné konanie,
  - poškodený,
  - zúčastnená osoba a
  - prokurátor

# ZNALECKÁ ČINNOSŤ

**V zmysle Zákona č 382/2004 Z.z. o znalcoch, tlmočníkoch a prekladateľoch:**

- Znalecká činnosť:
  - **špecializovaná odborná činnosť vykonávaná za podmienok ustanovených v zákone znalcami pre zadávateľa**
  - úlohou znalca je zodpovedať položené otázky v písomnom znaleckom posudku
  - znalec **nie je oprávnený vyjadrovať sa k právnemu posúdeniu veci**
  - v každom znaleckom úkone musí byť **odôvodnený postup** a musí byť zabezpečená jeho **preskúmateľnosť**.
- Znalec:
  - fyzická osoba alebo právnická osoba splnomocnená štátom na vykonávanie činnosti podľa zákona, ktorá je zapísaná v zozname znalcov, tlmočníkov a prekladateľov

# ZNALECKÉ ÚKONY



# ZNALECKÉ ODVETVIA RELEVANTNÉ Z HĽADISKA DFA

**10 00 00 Elektrotechnika**

- 10 01 00 Elektro-energetické stroje a zariadenia
- 10 02 00 Elektronika
- 10 03 00 Elektrotechnické materiály
- 10 04 00 Riadiaca technika, výpočtová technika (hardvér)
- 10 05 00 Robotické a mechatronické systémy
- 10 06 00 Elektronické komunikácie
- 10 07 00 Odhad hodnoty elektrotechnických zariadení
- 10 08 00 Nosiče zvukových a zvukovoobrazových záznamov
- 10 09 00 Počítačové programy (softvér)
- 10 10 00 Bezpečnosť a ochrana informačných systémov

**27 00 00 Písmoznalectvo**

- 27 01 00 Ručné písmo
- 27 02 00 Strojové písmo
- 27 03 00 Jazyková analýza

**49 00 00 Kriminalistika**

- 49 06 00 Kriminalistické skúmanie ručného písma a podpisov
- 49 08 00 Kriminalistické skúmanie dokumentov
- 49 20 00 Kriminalistická informatika
- 49 21 00 Kriminalistická fotografia a video

- Znalecké odvetvie kybernetická bezpečnosť **nie je vymedzené** v zákone o znalcoch
- KB je **komplexná disciplína,** ktorá si zvyčajne vyžaduje uplatnenie niekoľkých rôznych znaleckých odvetví

# TRESTNÉ KONANIE

**Trestné konanie**: je zákonom upravený postup orgánov činných v trestnom konaní a súdu, prípadne aj iných osôb zúčastnených na trestnom konaní

- V trestnom konaní treba dokazovať najmä:
  a) či sa stal skutok a či má znaky trestného činu,
  b) kto tento skutok spáchal a z akých pohnútok,
  c) závažnosť činu vrátane príčin a podmienok jeho spáchania,
  d) osobné pomery páchateľa v rozsahu potrebnom na určenie druhu a výmery trestu a uloženie ochranného opatrenia a iné rozhodnutia,
  e) následok a výšku škody spôsobenú trestným činom,
  f) výnosy z trestnej činnosti a prostriedky na jej spáchanie, ich umiestnenie, povahu, stav a cenu,
  g) majetkové pomery na účely odňatia výnosov z trestnej činnosti.

# DOKAZOVANIE

**§ 119 ods. 2 zákona č. 301/2005 Z. Z. Trestný poriadok:**

- Za dôkaz môže slúžiť všetko, čo môže prispieť na náležité objasnenie veci a čo sa získalo z dôkazných prostriedkov podľa zákona
- **Dôkazné prostriedky** sú najmä:
  - výsluch obvineného, svedkov, **alebo znalcov**
  - **posudky a odborné vyjadrenia**
  - previerka výpovede na mieste
  - rekognícia, rekonštrukcia, vyšetrovací pokus, obhliadka,
  - **veci a listiny dôležité pre konanie**
  - oznámenie, informácie získané použitím informačno-technických prostriedkov alebo prostriedkov operatívno-pátracej činnosti
- **Listinnými dôkazmi sú** listiny, ktoré svojím obsahom dokazujú alebo vyvracajú skutočnosť vzťahujúcu sa na objasňovaný skutok, na obvineného alebo iné osoby, ktoré majú k veci vzťah
- **Vecnými dôkazmi sú** predmety, ktorými alebo na ktorých bol trestný čin spáchaný, ktoré dokazujú alebo vyvracajú dokazovanú skutočnosť a môžu byť prostriedkom na odhalenie alebo zistenie trestného činu alebo jeho páchateľa, ako aj stopy trestného činu

# STOPA VS. DÔKAZ

- **Pojem DÔKAZ je nevyhnutné jasne odlíšiť od pojmu STOPA** (najmä v zmysle trestno-právnom)

- **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.
  [Straus, Vavera: Slovník kriminalistických pojmů a osobností, 2010, ISBN 978-80-7380-258-5]

- **Digitálne dôkazy**: informácie alebo údaje uložené alebo zasielané v binárnej forme, na ktoré sa možno opierať v dôkaznom konaní
  [ISO/IEC 27037]

- Žiaden dôkaz nemá predpísanú zákonnú silu

- Získaná „**digitálna stopa**" je typicky v dôkaznom konaní vykonaná ako vecný dôkaz podľa §153TP

# DOKAZOVANIE A DÔKAZNÉ PROSTRIEDKY

- **Dôkazné bremeno**: kľúčový pojem z hľadiska dokazovania. Rozumie sa tým zodpovednosť účastníka konania (či už navrhovateľa alebo odporcu) za to, že jeho tvrdenia budú v súdnom konaní skutočne preukázané a nebude tak rozhodnuté v jeho neprospech vtedy, keď určitá skutočnosť nemôže byť bez ďalšieho dôkazu preukázaná
- **Prípustnosť vykonania dôkazu**: Dôkaz získaný nezákonným donútením alebo hrozbou takého donútenia sa nesmie použiť v konaní okrem prípadu, keď sa použije ako dôkaz proti osobe, ktorá také donútenie alebo hrozbu donútenia použila. (Pokiaľ nie je spôsob vykonania dôkazu predpísaný, určí ho súd)
- **Negatívna dôkazná teória**: pravidlo, že neexistencia (niečoho) majúca trvajúci charakter sa zásadne nepreukazuje. (Na nikom nemožno spravodlivo žiadať, aby preukázal neexistenciu určitej právnej skutočnosti)

# TECHNICKÉ NORMY O DFA

- Problematiku digitálnych stôp a digitálneho dokazovania pokrýva technická norma ***ISO/IEC 27037:2012*** *Information technology -- Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital evidence*
  - Uplatňovanie tejto medzinárodnej normy si vyžaduje súlad s národnou legislatívou, pravidlami a reguláciou
  - Nemala by nahradzovať konkrétne právne požiadavky ktorejkoľvek jurisdikcie
  - Môže poslúžiť ako praktické usmernenie pri vyšetrovaniach ktoré sa týka digitálnych stôp
  - Nevzťahuje sa na spôsob analýzy digitálnych dôkazov
  - Nenahrádza špecifické požiadavky ako prípustnosť dôkazov, váhu dôkazov, relevantnosť dôkazov a iné súdom stanovené obmedzenia vzťahujúce sa na používanie potenciálnych digitálnych dôkazov pred súdom.
- Aby sa zachovala integrita digitálnych dôkazov, od používateľov tejto normy sa vyžaduje, aby upravili a zmenili postupy dokazovania opísané v norme v súlade s právnymi požiadavkami konkrétnej jurisdikcie

# ZÁSADY DIGITÁLNEHO DOKAZOVANIA

Vo väčšine jurisdikcií a organizácií sa digitálne dokazovanie riadi tromi základnými princípmi:

- **Relevancia** - malo by byť možné preukázať, že získané dáta sú relevantné pre vyšetrovanie - t.j. že obsahujú informácie, ktoré majú význam pri analýze konkrétneho incidentu, a že existuje dobrý dôvod, prečo boli získané
- **Spoľahlivosť** - všetky procesy používané pri manipulácii s potenciálnymi digitálnymi dôkazmi by mali byť kontrolovateľné a opakovateľné. Výsledky aplikácie takýchto procesov by mali byť reprodukovateľné.
- **Dostatočnosť** – analytik by mal sa mal ubezpečiť, že bolo zhromaždených dostatok údajov, aby bolo možné vykonať riadne vyšetrovanie

# SPRACOVANIE DIGITÁLNYCH STÔP

Existujú štyri kľúčové aspekty pri spracovávaní potenciálnych digitálnych dôkazov:

1. **Preskúmateľnosť**: nezávislému hodnotiteľovi by malo byť umožnené, aby posúdil činnosti, ktoré vykonal analytik, s cieľom určiť, či bola dodržaná vhodná vedecká metóda, technika alebo postup
   - Overiteľnosť sa dá umožniť najmä prostredníctvom vhodného zdokumentovania všetkých vykonaných krokov
2. **Opodstatnenosť**: analytik by mal byť schopný zdôvodniť všetky činnosti a metódy používané pri spracovaní digitálnych stôp.
   - Opodstatnenosť môže byť dosiahnutá tým, že sa preukáže, že rozhodnutie bolo najlepšou voľbou na získanie všetkých stôp ako potenciálnych digitálnych dôkazov
3. **Opakovateľnosť**: je uplatnená, ak sú rovnaké výsledky testov dosiahnuté za podmienky použitia rovnakého postupu a metódy merania, použitia rovnakých nástrojov a keď test môže byť opakovateľný kedykoľvek po pôvodnom teste
   - Odborne kvalifikovaní a skúsení analytici by mali byť schopní vykonať všetky procesy opísané v dokumentácii a dospieť k rovnakým výsledkom bez usmernenia alebo dodatočnej interpretácie
4. **Reprodukovateľnosť**: je uplatnená, ak sú rovnaké výsledky testov dosiahnuté za podmienky použitia rovnakej metódy merania, použitia rôznych nástrojov a rôznych podmienok, a keď test môže byť reprodukovateľný kedykoľvek po pôvodnom teste
   - Potreba reprodukovať výsledky sa líši podľa jurisdikcií a okolností, takže osoba, ktorá robí reprodukciu, musí byť informovaná o príslušných podmienkach

# IDENTIFIKÁCIA DIGITÁLNYCH STÔP

- Digitálne dôkazy sú reprezentované vo fyzickej aj logickej forme:
  - Fyzická forma zahŕňa zobrazenie údajov na rozhraní konkrétneho zariadenia
  - Logická forma potenciálneho digitálneho dôkazu sa týka virtuálneho zobrazenia a interpretácie údajov
- **Zhromažďovanie:** je proces spracovania stôp, v ktorom sú zariadenia, ktoré môžu obsahovať potenciálne digitálne dôkazy, odstránené z pôvodného umiestnenia a prenesené do laboratória alebo do iného kontrolovaného prostredia na neskoršiu analýzu
- **Akvizícia** (získanie): zahŕňa vytvorenie kópie digitálnych dôkazov (napr. kompletný pevný disk, oddiel, vybrané súbory, dump) a dokumentovanie použitých metód a vykonaných činnost

# AKVIZIČNÝ PROCES

- Analytik by mal **získať potenciálne digitálne dôkazy najmenej rušivým spôsobom**, aby sa zabránilo ich zmenám. Ak by proces mal viesť k neodvratnej zmene údajov, vykonané činnosti by mali byť zdokumentované, aby sa tieto zmeny zohľadnili.
- Optimálne by sa mala vytvoriť **digitálna dôkazová kópia digitálnych stôp alebo digitálnych zariadení**, ktoré môžu obsahovať potenciálne digitálne dôkazy.
- Originálny zdroj aj **kópia digitálnych dôkazov by mali byť overené s preukázateľnou verifikačnou funkciou**, ktorá je prijateľná pre osobu, ktorá bude dôkazy využívať. Pôvodný zdroj a každá kópia digitálnych dôkazov by mali produkovať rovnaký výstup verifikačnej funkcie.
- Môžu existovať prípady, v ktorých nie je možné alebo prípustné vytvoriť kópiu digitálneho dôkazu zdroja dôkazov, napríklad keď je zdroj údajov príliš objemný. V týchto prípadoch môže analytik vykonať logickú akvizíciu, ktorá sa zameriava iba na konkrétne dátové typy, adresáre alebo lokality. Toto spravidla prebieha na úrovni súborového systému resp. diskových oddielov.
- Niektoré jurisdikcie môžu vyžadovať špeciálne zaobchádzanie s údajmi; napríklad zapečatiť ju za prítomnosti vlastníka údajov. Zapečatenie by malo byť vykonané v súlade s miestnymi požiadavkami (legislatívnymi a procedurálnymi)

# VOLATILITA DIGITÁLNYCH STÔP

- Digitálne stopy sú typicky volatilného (krehkého) charakteru
  - Nesprávnym skúmaním môžu byť zmenené, manipulované alebo zničené
- Spracovatelia by preto mali byť spôsobilí na identifikáciu a zvládnutie rizík a dôsledkov možných postupov pri získavaní digitálnych stôp
  - Nedostatočné zvládnutie zariadení môže spôsobiť, že potenciálne digitálne dôkazy obsiahnuté v týchto zariadeniach sa stanú nepoužiteľnými.
- Analytici by mali dodržiavať zdokumentované postupy na zabezpečenie zachovania integrity a spoľahlivosti potenciálnych digitálnych dôkazov
- Postupy by mali obsahovať pokyny na spracovanie zdrojov potenciálnych digitálnych dôkazov a mali by obsahovať tieto základné zásady:
  - Minimalizovať manipuláciu s pôvodným digitálnym zariadením alebo potenciálnym digitálnym dôkazom
  - Zohľadniť všetky vykonané zmeny a dokumentovať vykonané kroky
  - Dodržiavať lokálne pravidlá dôkazného konania
  - Nevykonávať aktivity nad rámec vlastných spôsobilostí

# UCHOVANIE ZÍSKANÝCH STÔP

- Potenciálne digitálne dôkazy by mali byť zachované tak, aby sa zabezpečila ich použiteľnosť pri vyšetrovaní. Je dôležité **chrániť integritu dôkazov**
- Proces uchovávania zahŕňa ochranu digitálnych stôp a digitálnych zariadení, ktoré môžu obsahovať potenciálne digitálne dôkazy pred neoprávnenou zmenou alebo znehodnotením
  - Typicky je uchovanie riešené vytvorením bitového obrazu podozrivého disku pomocou overeného nástroja pre tvorbu digitálnych kópií s cieľom vytvoriť kópiu digitálnej stopy (napr. FTK Imager, podporované výstupné formáty: 01, S01, L01, AFF, AD1, RAW/DD)
- V ideálnom scenári by nemala existovať žiadna závislosť na samotných údajoch ani v metaúdajoch, ktoré sú s nimi spojené
- Analytik by mal byť schopný **preukázať, že digitálne stopy neboli zmenené od ich zberu alebo získania** (napr. pomocou použitia časových pečiatok a hash reportu)
- V niektorých prípadoch je dôvernosť potenciálnych digitálnych dôkazov požiadavkou, či už obchodnou alebo zákonnou (napr. ochrana súkromia)

# ZÁZNAM O REŤAZCI STAROSTLIVOSTI

Pri každom vyšetrovaní by analytik mal byť schopný zodpovedať za všetky získané údaje a zariadenia v čase, keď sú v jeho úschove.

- **Záznam o reťazci starostlivosti** (Chain of Custody Record) je dokument, ktorý identifikuje chronológiu pohybu a manipulácie s potenciálnymi digitálnymi dôkazmi.
- Tvorba záznamu by sa mala začať od procesu zberu alebo získavania. To je možné dosiahnuť sledovaním histórie položky od okamihu jej identifikácie, zhromaždenia alebo získania vyšetrovacím tímom až po súčasný stav a úložisko.
- Záznam o reťazci starostlivosti je dokument alebo séria súvisiacich dokumentov buď vo forme digitálnych údajov, alebo v iných formátoch (ako napríklad papierové poznámky).
- Záznam o reťazci starostlivosti musí obsahovať najmenej nasledovné údaje:
  - Jedinečný identifikátor získanej stopy (napr. identifikácia média, umiestnenie, sériové číslo, číslo modelu, MAC adresa, súvisiace IP adresy, atď.)
  - Zoznam osôb, ktoré pristupovali ku získaným stopám, čas a miesto prístupu
  - Zoznam osôb, ktoré kontrolujú pohyb potenciálnych dôkazov z úschovy a do úschovy a čas tohto presunu, od momentu keď digitálne zariadenie a / alebo potenciálne digitálne dôkazy boli získané
  - Typ aktivity, dôvod prečo boli potenciálne dôkazy vyzdvihnuté (vrátane účelu) a príslušný orgán, ak je to uplatniteľné
  - Všetky nevyhnutné zmeny potenciálnych digitálnych dôkazov, rovnako ako meno osoby zodpovednej teda aj zdôvodnenie pre zavedenie zmeny.
- Reťazec starostlivosti by mal byť zaručený po celú dobu životnosti dôkazov a byť uchovávaný po určitú dobu po skončení životnosti dôkazov.

# OPATRENIA NA MIESTE INCIDENTU

- Forenzný technik by mal vykonať činnosti na zabezpečenie a ochranu umiestnenia potenciálnych digitálnych dôkazov, ihneď po príchode na miesto.
- Činnosti by mali obsahovať nasledujúce úkony, v súlade s národnou legislatívou:
  - Zaistenie a prevzatie kontroly nad oblasťou v ktorej sa nachádzajú zariadenia
  - Určiť, kto je najvyššia zodpovedná osoba
  - Uistiť sa, že sa všetky osoby vzdialili od zariadení a zdrojov napájania
  - Legitimovať každého, kto má prístup k lokácii a každého, kto by mohol mať dôvod byť prítomný na mieste incidentu
  - V prípade, že je zariadenie zapnuté nevypínať ho a ak je zariadenie vypnuté nezapínať ho
  - Pokiaľ je to možné, zdokumentovať (napr. zakresliť, odfotografovať) scénu, všetky komponenty a kabeláže v ich pôvodnej polohe. Označiť porty a káble tak, aby konfigurácia systému mohla byť zrekonštruovaná neskôr
  - Ak je to možné, prehľadať priestor či sa v ňom nevyskytujú také položky, ako sú lístky s poznámkami, denníky, doklady, zápisníky, alebo hardvérové a softvérové príručky so zásadnými detailami o zariadení (napr. heslá a PIN čísla)

# MINIMÁLNE OPATRENIA

- Základné činnosti by mali byť vykonávané vždy, i keď zdanlivo nie je dôvod. Tento prístup sa označuje ako **prijatie minimálnych opatrení:**
  - S cieľom zabezpečiť správnu identifikáciu by mal **analytik označiť všetky potenciálne digitálne dôkazy štítkami**. (Niektoré jurisdikcie majú špecifické požiadavky na formát označovania dôkazného materiálu).
  - Štítok by nemal byť umiestnený priamo na mechanických častiach digitálnych zariadení a nemal by prekrývať alebo skrývať dôležité identifikačné znaky.
  - Všetky potenciálne digitálne dôkazy a zhromaždené zariadenia musia byť **získané a uložené takým spôsobom, aby bola zaistená integrita** dôkazov
  - Prístroje, ktoré sú pripojené k batériám a ktoré obsahujú **volatilné dáta, je potrebné pravidelne kontrolovať** a zabezpečiť, že zariadenia majú vždy dostatočné napájanie
  - Počítače a digitálne zariadenia by mali byť **zabalené takým spôsobom, aby nedošlo k poškodeniu nárazmi, vibráciami, vysokou nadmorskou výškou, teplom a vystaveniu elektromagnetickému žiareniu** počas prepravy
  - Magnetická záznamové médiá by mali byť **uložené v obale, ktorý je magneticky inertný, antistatický** a bez nečistôt
  - Digitálne zariadenia môžu obsahovať aj latentné stopy alebo biologické dôkazy. V tom prípade je je potrebné vykonať také kroky, aby sa zachovali potenciálne digitálne dôkazy - vytvorenie bitového obrazu digitálnych dôkazov by sa malo uskutočniť až po zhromaždení latentných stôp, alebo biologických dôkazov ktoré bolo vykonané na zariadení

# Záver

OVEROVANIE ÚROVNE KYBERNETICKEJ BEZPEČNOSTI

# Hlavné zásady znaleckých úkonov

- Samotná digitálna stopa ešte nie je dôkazom; aby sa stopa mohla stať potenciálnym dôkazom, je nutné **dbať na splnenie určitých podmienok** pri identifikácii, zbere, získavaní a uchovaní stôp, najmä:
  - prijať minimálne opatrenia pre narábanie so získanými digitálnymi stopami
  - vytvoriť digitálnu dôkazovú kópiu digitálnych stôp alebo digitálnych zariadení, vrátane verifikácie (Hash)
  - uplatniť primeranú starostlivosť o získané digitálne stopy
  - zabezpečiť záznam o reťazci starostlivosti (Chain of Custody Record)
- Dôkaz získaný nezákonným donútením alebo hrozbou donútenia sa nesmie použiť v konaní
- Platí tzv. negatívna dôkazná teória: neexistencia (niečoho) sa zásadne nepreukazuje. (Nemožno preukázať neexistenciu určitej právnej skutočnosti)
- Dôkazné prostriedky musia byť r**elevantné** pre vyšetrovanie, **spoľahlivé (**t.j. najmä preskúmateľné, opakovateľné a reprodukovateľné) a **dostatočné,** (aby bolo možné vykonať riadne vyšetrovanie)
- Pri spracovávaní potenciálnych digitálnych dôkazov je potrebné myslieť na 4 kľúčové zásady:
  1. **Preskúmateľnosť**: nezávislý analytik musí byť schopný posúdiť použitú vedeckú metódu, techniku alebo postup
  2. **Opodstatnenosť**: analytik musí byť schopný zdôvodniť všetky činnosti a metódy používané pri spracovaní digitálnych stôp
  3. **Opakovateľnosť**: možnosť dosiahnuť rovnaké výsledky DFA pri použití rovnakého postupu a rovnakých nástrojov
  4. **Reprodukovateľnosť**: možnosť dosiahnuť rovnaké výsledky DFA pri použití použitia rôznych nástrojov a rôznych podmienok oproti pôvodnému testu

# Hlavné zásady auditu kybernetickej bezpečnosti

- **Zásada etiky** - Audítor kybernetickej bezpečnosti má vykonávať audit poctivo a zodpovedne, objektívnym a nezaujatým spôsobom. Kdekoľvek je to možné, audítor má byť nezávislý od objektu posudzovania a má vo všetkých prípadoch konať spôsobom, ktorý vylúči tendenčnosť a konflikt  záujmov.
- **Prístup založený na dôkazoch** - Musia byť použité racionálne metódy, ktorých cieľom je v systematickom procese auditovania dosiahnuť spoľahlivé a reprodukovateľné závery auditu
- **Procesný prístup** - Výsledky auditu sa dosiahnu efektívnejšie, ak audítor pochopí procesy PZS a ich celkové vzájomné pôsobenie ako súvisiacich činností ktoré sú vykonávané ako kompaktný, holistický systém
- **Prístup založený na riziku** - Audit má byť zameraný na skutočnosti významné pre dosiahnutie cieľov programu auditu, berúc do úvahy identifikované riziká a opatrenia primerané rizikám
- **Zásada relevantnosti** - Audítor má vedieť preukázať, že získané dôkazy sú relevantné pre audit - t.j. že obsahujú informácie, ktoré majú význam pre posúdenie a že existuje dobrý dôvod, prečo boli získané.
- **Zásada úplnosti a správnosti** - Audítor je zodpovedný, že všetky dôkazy, ktoré získa a používa počas auditu sú správne a úplne. Všetky získané auditné dôkazy musia byť uchované, aby sa ku rovnakým výsledkom vedel dostať aj iný a nezávislý audítor pri opakovanom výkone auditu.
- **Zásada proporcionality** - Zásada proporcionality upravuje, ako má audítor vykonávať svoje právomoci. Podľa zásady proporcionality platí, že audítor podnikne na dosiahnutie cieľov auditu kroky len v takom rozsahu, ktoré sú nevyhnutné na dosiahnutie daného cieľa.
- **Zásada primeranej starostlivosti** Audítor sa musí vyhnúť akýmkoľvek aktivitám, ktoré by mohli viesť k znehodnoteniu potenciálnych dôkazov na základe úmyselného či neúmyselného konania. Audítor napríklad nesmie pristupovať ku zariadeniam, ak nemá potrebné schopnosti a nie je pripravený využiť spoľahlivé a overené postupy.

# Kto sa môže stať audítorom kybernetickej bezpečnosti?

**§ 29 Zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti:**

- Audit kybernetickej bezpečnosti vykonáva **certifikovaný audítor kybernetickej bezpečnosti,** ktorým je fyzická osoba, spoločník, štatutárny orgán alebo zamestnanec právnickej osoby
- Certifikáciu audítora kybernetickej bezpečnosti vykonáva akreditovaný orgán certifikujúci osoby v oblasti kybernetickej bezpečnosti
- Kvalifikačné požiadavky sú uvedený vo Vyhláške Národného bezpečnostného úradu č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora:
  - audítor spĺňa podmienky znalostného štandardu podľa prílohy č. 1 overené skúškou doloženou podľa odporúčaní medzinárodne akceptovaných technických noriem alebo iných, týmto štandardom vecne obdobných a všeobecne uznávaných postupov
  - Napr: pre vysokoškolské vzdelanie druhého stupňa:
    - skúsenosti v oblasti informačných technológií kybernetickej bezpečnosti - **najmenej päť rokov praxe**
    - životopis s uvedením kontaktu na overiteľnú referenciu
    - **zoznam vykonaných auditov** s uvedením kontaktu na overiteľnú referenciu
    - skúsenosti v oblasti auditu informačných systémov - **najmenej tri roky praxe**
    - medzinárodný certifikát z oblasti auditu informačných systémov (CISA, LA27k)

# Kto sa môže stať súdnym znalcom?

**§ 2 a § 5 382/2004 Z. z. o znalcoch, tlmočníkoch a prekladateľoch**

- Znalec, tlmočník alebo prekladateľ je fyzická osoba alebo právnická osoba splnomocnená štátom na vykonávanie činnosti podľa tohto zákona, ktorá je:
  - zapísaná v zozname znalcov, tlmočníkov a prekladateľov a ktorá:

a) je spôsobilá na právne úkony v plnom rozsahu,

b) je bezúhonná,

c) získala **vzdelanie v odbore**; v prípade znalcov **vysokoškolské vzdelanie druhého stupňa** v študijnom odbore zameranom na odbor alebo odvetvie, ktoré je predmetom písomnej žiadosti o zápis, inak najvyššie vzdelanie, ktoré je možné získať v danom odbore,

d) úspešne skončila osobitné vzdelávanie o spôsobe výkonu činnosti podľa tohto zákona (ďalej len „**odborné minimum**"),

e) po získaní vzdelania v odbore vykonáva prax v odbore, ktorý je predmetom činnosti, v trvaní **najmenej sedem rokov**,

f) zložila skúšku z odboru alebo odvetvia, ktoré je predmetom žiadosti o zápis a ktorou preukazuje svoju odbornú spôsobilosť (ďalej len „**odborná skúška**"),

g) úspešne skončila **špecializované vzdelávanie**, ak ide o zapísanie do zoznamu pre odbor alebo odvetvie, v ktorom je také vzdelávanie ustanovené všeobecne záväzným právnym predpisom [§ 33 písm. b)],

h) má **materiálne vybavenie** postačujúce na výkon činnosti v odbore alebo odvetví, ktoré je predmetom písomnej žiadosti o zápis,

i) nebola v posledných troch rokoch právoplatne vyčiarknutá zo zoznamu podľa § 26 ods. 3 písm. c) alebo jej neplynie zákaz výkonu činnosti podľa § 26 ods. 3 písm. b),

j) **zložila sľub**

# Všeobecný účel digitálnej forenznej analýzy a overovania kybernetickej bezpečnosti

## AUDIT KYBERNETICKEJ BEZPEČNOSTI

- získať objektívnu informáciu o stave ochrany informácií, najmä:
  - Zhodnotiť:
    - Aktuálny stav kybernetickej bezpečnosti
    - Súlad  prijatých opatrení so stanoveným rozsahom opatrení
    - Účinnosť implementovaných bezpečnostných opatrení
    - Bezpečnostnú architektúru (napr. tzv. „security by design" podľa GDPR)
    - Vyspelosť procesu riadenia bezpečnosti
  - Identifikovať zraniteľnosti a hrozby a stanoviť úrovne rizík
  - Atestovať spôsobilosti organizácie v oblasti kybernetickej bezpečnosti

## ZNALECKÝ ÚKON

- dôveryhodným spôsobom získať a uchovať relevantné, spoľahlivé a dostatočné dôkazy použiteľné v ďalšom konaní:
  - vo vyšetrovaniach a súdnych sporoch
  - v pracovno-právnych vzťahoch

NCC-SK
SLOVAKIA CYBERSECURITY COORDINATION CENTRE




Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autorov a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za nich nepreberajú žiadnu zodpovednosť.