Popis Slovníku kybernetické bezpečnosti

(Cyber security glossary) v prostředí SW ATOM

Obsah:

[1. Cíl 1](#_Toc137141030)

[2. Struktura (ontologie) 1](#_Toc137141031)

[3. Třídy (classes) a vztahy (associations) 2](#_Toc137141032)

[4. Třídy a atributy (attributes) 2](#_Toc137141033)

[5. Číselníky 2](#_Toc137141034)

[6. AREA 3](#_Toc137141035)

[7. CONCEPT 3](#_Toc137141036)

[8. DEFINITION 4](#_Toc137141037)

[9. SOURCE 4](#_Toc137141038)

[10. Potenciální rozvoj slovníku 4](#_Toc137141039)

[11. Metodika a postup práce 4](#_Toc137141040)

[12. Rozvoj slovníku o další jazykové mutace 5](#_Toc137141041)

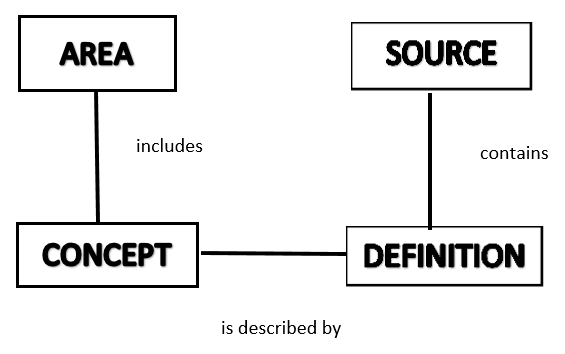
[13. Přístupový portál ke Slovníku 5](#_Toc137141042)

# Cíl

Vytvořit znalostní systém vybraných pojmů (CONCEPT) kybernetické bezpečnosti, tím usnadnit jejich studium a využití ve výzkumu. Pojmy vytvořit integrací jejich definic (DEFINITION) z několika zdrojů (SOURCE) a to nejprve v češtině. Slovník má potenciál rozvoje k podpoře libovolného národního jazyka; nejprve slovenštiny, případně další jazyky států Visegrádské 4 (polština, maďarština). Nástrojem pro tvorbu slovníku je SW ATOM, společnosti AION CS, Zlín. Slovník je na adrese: [**https://unob.atom3.cz**](https://unob.atom3.cz) ; Ontology: **Cyber security glossary**; přístupové údaje: **guest / guest**.

# Struktura (ontologie)

Struktura znalostního systému zahrnuje třídy, atributy a vztahy. Koncepční návrh je uveden na obr. 1.



Obrázek Koncepční návrh tříd a vztahů ontologie

# Třídy (classes) a vztahy (associations)

**AREA** – zahrnuje oblast pojmů daného tématu a charakteristiky. Basename vyjadřuje podrobně oblast.

**CONCEPT** – pojem z kybernetické bezpečnosti (zde jako výsledek studia a integrace). Basename = pojem.

**DEFINITION** – definice pojmu podle zdroje. Basename je sestaveno mnemonicky: pojem\_zkratka zdroje.

**SOURCE** – zdroj definice pojmu. Typ zdroje je přiřazen z číselníku v ATOMu. Basename je sestaveno mnemonicky: zkratka zdroje\_stát (NATO country code).

Tabulka Vztahy mezi třídami

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Třída1** | **Třída2** | **Vztah** | **Role T1** | **Role T2** |
| AREA | CONCEPT | includes | contains a concept | belongs to the area |
| CONCEPT | DEFINITION | is described by | is defined by | definition of a concept |
| SOURCE | DEFINITION | contains | source of definition | included in the source |

# Třídy a atributy (attributes)

BASENAME – identifikátor výskytu třídy v ATOMu, většinou sestaven mnemonicky pro snadnou identifikaci v sadě výskytů stejné třídy. Musím být unikátní.

Tabulka Přiřazení atributu do třídy

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Atribut** | **Data type** | **AREA** | **CONCEPT** | **DEFINITION** | **SOURCE** |
| Abbreviation | Name | **X** |  |  | **X** |
| Annotation | Text |  |  |  | **X** |
| Note-ENG | Variant/String |  | **X** | **X** |  |
| Note-CZE | Variant/String |  | **X** | **X** |  |
| Note-SVK | Variant/String |  | **X** | **X** |  |
| Note-HUN | Variant/String |  | **X** | **X** |  |
| Note-POL | Variant/String |  | **X** | **X** |  |
| Source-classification | Group-tree |  |  |  | **X** |
| Integration-team-cze | Group-tree |  | **X** |  |  |
| Title-ENG | Name | **X** | **X** | **X** | **X** |
| Title-CZE | Name | **X** | **X** | **X** | **X** |
| Title-SVK | Name | **X** | **X** | **X** | **X** |
| Title-HUN | Name | **X** | **X** | **X** | **X** |
| Title-POL | Name | **X** | **X** | **X** | **X** |
| Text-ENG | Text | **X** | **X** | **X** |  |
| Text-CZE | Text | **X** | **X** | **X** |  |
| Text-SVK | Text | **X** | **X** | **X** |  |
| Text-HUN | Text | **X** | **X** | **X** |  |
| Text-POL | Text | **X** | **X** | **X** |  |
| Internet-address-source | Variant/Url |  |  |  | **X** |
| Source document | File |  |  |  | **X** |

# Číselníky

## Source-classification

Typ zdroje CZE: zákon, směrnice, kniha, článek v časopise, publikace na konferenci, prezentace na konferenci/webináři, strategický dokument.

Type of source ENG: law, guide, book, journal article, conference paper, conference/webinar presentation, strategic document.

## Integration-team-cze

Tým, který vytvořil CONCEPT z Univerzity obrany (UNOB): JB/UNOB (Jan Beran), LH/UNOB (Lubomír Horský), LB/UNOB (Ladislav Buřita). Postupně bude doplněn o týmy pro další spolupracující státy.

# AREA

Pro kategorizaci pojmů kybernetické bezpečnosti existuje řada taxonomií, sestavená z různých hledisek.

Naše vlastní taxonomie kategorizuje oblasti Slovníku kybernetické bezpečnosti verze 2, následovně:

* Strategické/obecné pojmy (Strategic-common concepts). STRATEG
* Organizace, orgány, funkce (Organizations-bodies-functions) ORG-FUN
* Chráněná aktiva (Protected assets). ASSETS
* Hrozby a útoky – obecně (Threats and attacks-general). THR-ATT\_GEN
* Hrozby a útoky – škodlivý SW (Threats and attacks-malware). THR-ATT\_MAL
* Hrozby a útoky – napadení sítě (Threats and attacks-network). THR-ATT\_NET
* Hrozby a útoky – napadení web.aplikací (Threats and attacks-web-applic). THR-ATT\_WEB
* Kybernetická obrana - metody,postupy,návody (Cyber defence-met, proc, instr) CYB-DEF\_MET
* Kybernetická obrana - nástroje (Cyber defence-tools) CYB-DEF\_TOOL

Přehled oblastí a pojmů je zpracován do tabulky Excel. Basename je název oblasti zájmu (area) v AJ.

## Strategické/obecné pojmy

Zahrnuje obecné a významné pojmy kybernetické bezpečnosti, které nepřísluší do ostatních oblastí.

It includes general and important concepts of cyber security that do not belong in other areas.

## Organizace, orgány, funkce

Obsahuje organizace, orgány a funkce spojené s kybernetickou bezpečností.

It contains organizations, bodies, and functions related to cyber security.

## Chráněná aktiva

Zahrnuje aktiva, která je třeba chránit před kybernetickými hrozbami a útoky.

It includes assets that need to be protected from cyber threats and attacks.

## Hrozby a útoky – obecně

Pojmy zahrnující kybernetické hrozby a útoky, které nespadají do dalších detailních oblastí.

Terms covering cyber threats and attacks that do not fall into other detailed areas.

## Hrozby a útoky – škodlivý SW

Kybernetické hrozby a útoky, které využívají škodlivý SW (malware).

Cyber threats and attacks that use malicious SW (malware).

## Hrozby a útoky – napadení sítě

Kybernetické hrozby a útoky na počítačovou síť. Cyber threats and computer network attacks.

## Hrozby a útoky – napadení webových aplikací

Kybernetické hrozby a útoky na webové aplikace. Cyber threats and attacks on web applications.

## Kybernetická obrana - metody, postupy, návody

Metody, postupy, návody kybernetické obrany. Cyber defense – methods, procedures, and instructions.

## Kybernetická obrana - nástroje

Nástroje kybernetické obrany. Cyber defense tools.

# CONCEPT

Vybraný pojem kybernetické bezpečnosti, jako výsledek analýzy definic a jejich integrace v národním jazyce a ENG. Přehled je v tabulce pojmů (Příloha Popisu). Basename je název pojmu v AJ.

# DEFINITION

Definice pojmu podle daného zdroje. Je uvedena v národním jazyce a ENG.

Pro vybrané pojmy se definice nezjišťují; např. pro konkrétní organizace.

Basename zahrnuje pojem\_zkratka-zdroje.

# SOURCE

Třída SOURCE zahrnuje literární zdroje definici pojmů, ale i další podklady pro tvorbu slovníku.

Basename: Název zdroje v AJ\_kód státu. Po uzavření první verze slovníku bylo evidováno 23 literárních zdrojů, z nichž nejčetnější využití pro definice pojmů slovníku měly:

1. **Výkladový slovník kybernetické bezpečnosti, Národní centrum kyber. a informační bezpečnosti.**Policejní akademie ČR a Česká pobočka AFCEA za aktivní podpory pracovníků Národního bezpečnostního úřadu ČR, Národního centra kybernetické bezpečnosti a odborné veřejnosti vydaly druhé, rozšířené vydání slovníku kybernetické bezpečnosti doplněné o anglický překlad českého výkladu odborných výrazů. Druhé, rozšířené vydání slovníku je publikováno v tištěné i elektronické PDF verzi pod ISBN 978-80-7251-397-0.  
   Jirásek, Petr, Novák, Luděk, and Požár, Josef. (2013). Výkladový slovník kybernetické bezpečnosti (Cyber Security Glossary). The National Cyber and Information Security Agency of the Czech Republic. Available at https://www.govcert.cz/cs/informacni-servis/akce-udalosti/2193-vykladovy-slovnik-kyberneticke-bezpecnosti-druhe-vydani/  
   **Basename**: Cyber Security Glossary of the National Cyber and Information Security Agency\_CZE.
2. **Glossary of Key Information Security Terms, National Institute of Standards and Technology, U.S.** Department of Commerce & **Glossary** only consists of terms and definitions extracted verbatim from **NIST's cybersecurity**- and privacy-related publications--Federal Information Processing Standards (FIPS), NIST Special Publications (SPs), and NIST Internal/Interagency Reports (IRs)--as well as from Committee on National Security Systems (CNSS) Instruction CNSSI-4009. Only terms that are defined in final publications—not drafts—are included here. <https://csrc.nist.gov/glossary>.  
   **Basename**: Glossary of Key Information Security Terms\_USA.
3. **Technology Dictionary Technopedia, Kanada.  
   Basename**: Technology Dictionary\_Technopedia\_CAN.
4. **WIKI Encyklopedie právních záležitostí, politik, publikací, případů, zákonů, událost**í; Unicorn. CZE  
   **Basename**: The Law IT\_WIKI, UNICORN\_CZE.
5. Zdrojem jsou i zkratky států – **NATO Country Codes (trigram)**; <http://en.wikipedia.org/wiki/List_of_NATO_country_codes>   
   **Basename**: NATO Country Codes-trigram

# Potenciální rozvoj slovníku

Rozšíření na libovolný národní jazyk, nejprve ve spolupráci s AOS (SVK), pak v rámci Visegrádské 4 (POL, HUN). Ke slovníku lze v dalších fázích rozvoje Slovníku připojit metodiky, návody na postupy a řešení v tématu kybernetické bezpečnosti. Celý rozvoj slovníku může probíhat v budoucnosti cyklicky. Po aktualizaci na zvolenou jazykovou mutaci, lze přechozí mutace upravovat podle stavu rozpracovanosti slovníkových pojmů.

# Metodika a postup práce při rozvoji slovníku o novou jazykovou mutaci

Nejprve je třeba provést důkladnou analýzu slovníkových zdrojů pro rozvoj slovníku. V případě, že bude zjištěn zdroj definic slovníku se zvláštním významem (např. legislativa), může se vedení týmu rozhodnout o vložení takových definic bez úpravy a bez ohledu na již dříve vložené definice a vytvořené pojmy. Lze doporučit tuto operaci pro vedení týmu. ***Pokud byly získány minimálně 3 definice, pokračuje proces integrace definic.*** V případě, že nebyly nalezeny alespoň 3 definice, je třeba nalézt v Internetu další zdroj (SOURCE), ze kterého budou definice doplněny. Získaný zdroj je třeba do systému vložit. ***Proces integrace definic pojmu*** je vysoce tvůrčí činnost, při které buď vyberete nejlepší definici, nebo jich několik spojíte, případně upravíte do výsledné podoby definice pojmu, který pak vložíte jako výsledek (CONCEPT).

**U víceslovných (komplexních pojmů) není nutno dodržet pravidlo integrace z 3 definic.**

# Metodické postupy rozvoje slovníku o slovenskou jazykovou mutaci

Pro rozvoj nové jazykové mutace slovníku lze aplikovat 5 metodických postupů:

1. Překlad pojmu, bez definic.
2. Doplnění nové definice a pojmu zvláštního významu.
3. Aktualizace definice a pojmu (zvláštního významu SVK), který byl již součástí slovníku.
4. Překlad pojmu a definic pro daný pojem do požadovaného jazyka bez integrace.
5. Doplnění vlastní definice v daném jazyce, překlad stávajících definic pro daný pojem do požadovaného jazyka a jejich integrace.

## Překlad pojmu bez definic.

Některé pojmy nemají definice, jsou pouze v podobě CONCEPT (AREA 02); do pojmu (CONCEPT) se přidají pouze slovenské údaje.

## Doplnění definice a pojmu zvláštního významu

Metodický postup respektuje situaci, kdy v národním prostředí existuje zákon/y, které definují pojmy kybernetické bezpečnosti. Daný pojem není ještě ve slovníku. Většinou je sice uvedeno, že pojmy jsou specifikované vzhledem k platnosti zákona, ale přesto je třeba na takovou situaci brát zvláštní zřetel.

## Aktualizace definice a pojmu zvláštního významu

Metodický postup respektuje situaci, kdy v národním prostředí existuje zákon/y, které definují pojmy kybernetické bezpečnosti. Daný pojem je již součástí slovníku, a proto je aktualizován. V prostředí slovníku se doplní nová definice (DEFINITION) a ta je převedena do pojmu (CONCEPT), uvedenou v příslušném zákoně, jako zdroji pro definici.

## 12.4 Překlad pojmu a definic pro daný pojem do požadovaného jazyka bez integrace.

Jedná se o případ doplnění slovenských položek do pojmu (CONCEPT) a do všech příslušných definic (DEFINITION)slovníku do požadované jazykové mutace.

## 12.5 Překlad definic pro daný pojem do požadovaného jazyka a jejich integrace

Přeloží se stávající definice (DEFINITION) příslušného pojmu (CONCEPT) do požadovaného jazyka. Překlad provádíme buď na základě vlastních znalostí nebo pomocí internetových či papírových slovníků. Přidá se nová definice a výsledný pojem (CONCEPT) vznikne integrací přeložených definic.

# Přístupový portál ke Slovníku

Portál umožní snadný, otevřený (bez přihlášení) a uživatelský přívětivý přístup k pojmům Slovníku. Až bude Slovník obsahovat více jazykových mutací pojmů, začne přístup ke Slovníku výběrem jazyka. To teď lze přeskočit, protože jsou pojmy pouze v češtině (angličtina je ale jeho nutnou, integrující součástí).

## Přístup k pojmům přes oblast (AREA) Slovníku

Po výběru oblasti (AREA) bude zobrazen seznam odpovídajících pojmů (CONCEPT), ze kterého po výběru pojmu bude zobrazen jeho detailní obsah.

## Přístup k pojmům Slovníku přímo

Přístup může být řízen například na základě uvedeného prvního písmene pojmu (CONCEPT). Pak se zobrazí odpovídající seznam pojmů, ze kterého bude možné pojem prohlédnout, stejně jako v případě přístupu v podkapitole 13. 1; pak rovněž následně bude umožněn přístup k definicím (DEFINITION) a informačním zdrojům (SOURCE).

V Brně 15. 7. 2023, Prof. Ladislav Buřita