EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

jihomoravský kraj

# LEGISLATIVA

## Legislativa ČR a legislativa ČR vztažená k ochraně informací – úvod do KB

## Metodický list

Autor: Ing. Jiří Sedláček, Metodik: Mgr. Hana Hrádková

Recenzent: Ing. Lukáš Přibyl

Rok vydání: 2023

Legislativa ČR a legislativa ČR vztažená k ochraně informací – úvod do KB podléhá licenci CC BY-SA 4.0 International License (Offline use: http://creativecommons.org/licenses/by-nc-sa/4.0/).

# Obsah

1 Cíle ..... 3
2 Dovednosti ..... 3
3 Pracovní prostředí ..... 4
4 Použitý model ..... 4
5 Charakteristika cvičení ..... 4
5.1 Hlavní zásady ..... 4
5.2 Výhody ..... 5
5.3 Nevýhody ..... 5
6 Klíčové charakteristiky ..... 5
7 Zainteresované strany ..... 6
7.1 Soutěžící týmy ..... 6
7.1.1 Očekávání od členů týmů ..... 6
7.2 Moderátor, hodnotitel, pozorovatel ..... 6
7.2.1 Moderátor ..... 6
7.2.2 Hodnotitel ..... 6
7.2.3 Pozorovatel ..... 6
8 Průběh cvičení ..... 7
8.1 Události ..... 7
8.2 Odpovědi ..... 7
8.3 Diskuze ..... 7
8.4 Závěrečný debrief a vyhodnocení ..... 7
9 Osnova výuky ..... 8
Teoretická část ..... 8
Praktická část ..... 9
10 Input 1 - Právní normy ..... 9
10.1 Hierarchie právních norem podle právní síly ..... 9
10.1.1 Právní normy jsou hierarchicky členěny podle právní síly. Zde uvedené typy právních norem spojte spojnicí od norem s nejvyšší právní sílou po nejnižší s níže umístěnou pyramidou: ..... 9

10.2 Zákony ČR a právo EU ..... 10
10.2.1 Proč jsou zákony ČR ovlivněny právními akty EU? ..... 10
10.2.2 Jaké typy EU právních aktů ovlivnily ZoKB, VyKB a OOÚ? ..... 10
11 Input 2 - Účel a struktura ZoKB a VyKB ..... 12
11.1 Účel a struktura ZoKB ..... 12
11.1.1 Popište účel a strukturu ZoKB ..... 12
11.2 Kybernetický prostor ..... 13
11.2.1 Čím je z pohledu ZoKB tvořen kybernetický prostor (uveďte jeho součásti a paragraf včetně odstavce či písmene)? ..... 13
11.2.2 Pro kterou ze součástí kybernetického prostoru je určen speciální zákon (uveďte název součásti a číslo a název zákona)? ..... 13
11.2.3 Jaký paragraf a odstavec či písmeno ZoKB definují zajištění bezpečnosti, dostupnosti a spolehlivosti součástí kybernetického prostoru? ..... 13
11.2.4 Jak jsou dle ZoKB rozdělena bezpečnostní opatření? ..... 13
11.2.5 Jak je dle ZoKB zajištěna bezpečnost informací (uveďte paragraf, odstavec či písmeno)? ..... 14
Shrnutí a závěr ..... 15
Seznam použitých zdrojů ..... 16

# 1 Cíle

Uvedení všech cílů, kterých bude v rámci této úlohy dosaženo, dle Bloomovy taxonomie výukových cílů (viz. Příloha 1)

- Porozumět smyslu práva v rámci fungování státu.
- Pochopit hierarchii právních norem podle právní síly a vliv právních předpisů EU na právní předpisy ČR.
- Pochopit dopady legislativy EU na zákon o kybernetické bezpečnosti (dále jen ZoKB) a vyhlášku o kybernetické bezpečnosti (dále jen VyKB).
- Pochopit smysl a strukturu ZoKB a VyKB.
- Pochopit roli NÚKIB coby ústředního správního orgánu v oblasti kybernetické bezpečnosti.
- Pochopit ZoKB a VyKB ve vztahu ke konkrétní typově popsané organizaci.
- Pochopit proces identifikace uvedené povinné osoby podle vyhlášky č. 437/2017 Sb., o kritériích pro určení provozovatelů základních služeb.
- Aplikovat právo ČR do právních aktů právnické osoby.

- Naučit se pracovat s vyhláškou o kybernetické bezpečnosti.
- Naučit se pracovat s webem NÚKIB.
- Porozumět významu a smyslu důvěrnosti informací a osvojit si praktickou aplikaci.
- Prohloubit znalosti účastníků cvičení v oblasti kybernetické bezpečnosti.
- Umožnit účastníkům cvičení sdílení zkušeností a názorů, včetně tréninku týmové práce a spolupráce.
- Rozvoj analytického myšlení. Uvažování v souvislostech.

# 2 Dovednosti

- Pracovat se zákonnými předpisy relevantními k cvičenému tématu.
- Aplikovat legislativu ČR dle hierarchie právních hodnot podle právní síly do předpisové základny organizace.
- Aplikovat konkrétní ustanovení zákona o kybernetické bezpečnosti a prováděcích vyhlášek do hypotetické organizace.
- Pracovat s webem NÚKIB.
- Vyjednávat v týmu o řešeních stanovené problematiky.
- Sdílet v týmech názory, znalosti a stanoviska.

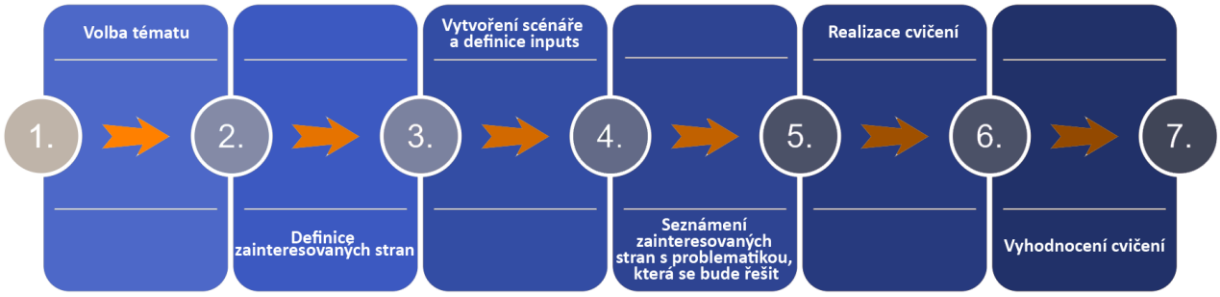
# 3 Pracovní prostředí

- Úlohu lze realizovat v učebně vybavené výpočetní technikou, tabulí s popisovači, projektorem a místem pro jednotlivé týmy.

Pro práci jsou vhodné následující pomůcky:

- Psací potřeby.
- Poznámkové bloky.
- Dle potřeb popisovací lepíky.
- Projektor s promítacím prostorem (plátno/stěna).
- Počítač s rozhraním pro připojení projektoru.

# 4 Použitý model




# 5 Charakteristika cvičení

Tabletop cvičení je druh tréninku, při němž je možné celkem nenákladnou formou procvičit navozená témata, včetně organizačních a technických opatření a znalostí k tomu potřebných. Cvičení je realizováno účastí jednotlivých týmů tzv. „u stolu“.

## 5.1 Hlavní zásady

- Týmový duch.
- Soutěživost.
- Spolupráce.
- Sdílení znalostí.
- Brainstorming.
- Rovnost názorů.

## 5.2 Výhody

- Nízko stresové prostředí.
- Nízké náklady.
- Průběžné hodnocení.
- Moderovaná skupinová diskuse o problémových oblastech.

## 5.3 Nevýhody

- Chybí reálný prožitek.
- Nejedná se o skutečný test provozní schopnosti.
- V rámci simulace je poskytnut pouze povrchní pohled na danou organizaci.

# 6 Klíčové charakteristiky

- Tento typ cvičení slouží k seznámení zúčastněných osob se související tématikou a k řešení navozené situace či témat. Cílem není hodnotit správnost odpovědí.
- V rámci týmu jsou určeny role a to tak, aby bylo cvičení co nejpřínosnější.
- Navozená situace či řešená témata vyžadují efektivní týmové rozhodování, a to navzdory nedostatku informací a časovému tlaku.
- Přínosnou a žádanou je diskuze, a to jak v týmech, tak i mezi týmy. Vede nejen k učinění relevantního rozhodnutí, ale je i přínosem cvičení.
- Každému rozhodnutí je vhodné předřadit relevantní faktory/roviny (bezpečnostní, věcné, právní, politické, ekonomické, mediální…).
- Navozená situace nemusí být vždy smyšlená. Může být inspirována skutečnou událostí.
- Scénář může popisovat děj podobný ději v reálném světě, v ČR, ve smyšlené organizaci.
- Je žádoucí řešit vždy pouze navozenou situaci či témata.

# 7 Zainteresované strany

## 7.1 Soutěžící týmy

- Cvičení se zúčastní 4 týmy po 5 členech.
- V tomto konkrétním cvičení se nerozlišují role jednotlivých aktérů s výjimkou určení zástupce za každý tým pro komunikaci jménem týmu.
- Týmy mají k dispozici tento manuál a další materiály potřebné k účasti na cvičení – viz níže.

### 7.1.1 Očekávání od členů týmů

Nezdráhejte se zapojit do konverzace. Buďte aktivní, vyzývejte i ostatní členy týmu k zapojení do diskuze. Je v pořádku nemít odpověď. Přijměte představený scénář a pracujte v rámci uvedených parametrů.

## 7.2 Moderátor, hodnotitel, pozorovatel

### 7.2.1 Moderátor

- Zástupce školy, případně externí spolupracovník.
- Moderátor má k dispozici tento manuál a materiály s klíčem k řešení událostí a inputs.

#### 7.2.1.1 Činnosti moderátora

- Seznámí týmy se scénářem/tématy.
- Řídí čas.
- Operativně reaguje v rámci nastalé situace atd.
- Kontrolujte tempo a průběh cvičení.
- Stimulujte a řídí diskusi.
- V případě potřeby dodává vodítka.
- Získává odpovědi a řešení od týmů.

### 7.2.2 Hodnotitel

- Zástupce školy, případně externí spolupracovník.
- Hodnotitel je seznámen s navozeným tématem či situací v rámci daného cvičení.

#### 7.2.2.1 Činnosti hodnotitele

- U Týmů identifikujte silné stránky a oblasti zlepšení.
- Pomáhá vypracovat zprávu po cvičení.

### 7.2.3 Pozorovatel

- Zástupce školy, případně externí spolupracovník.
- Pozorovatel je seznámen s navozeným tématem či situací v rámci daného cvičení.

#### 7.2.3.1 Činnosti pozorovatele

- Účastní se diskuze, pokud je požádán.

***Pozn.: Pro potřeby cvičení, v prostředí organizace typu střední škola, je možné, s cílem snížení nároků na personální zdroje, role moderátora, hodnotitele a pozorovatele sloučit do jedné role.***

# 8 Průběh cvičení

## 8.1 Události

- Scénář cvičení je koncipován tak, že dané téma je řešeno v několika oddělených vstupech (inputs – viz materiál pro týmy). Ta budou vždy moderátorem představena ať už ústně či za pomoci prezentace.
- V rámci každého inputu obdrží každý tým otázky, případně formulář pro zaznamenání odpovědí. Otázky mohou být doplněny i grafickými informacemi. Vše je nutné pečlivě přečíst a zanalyzovat.
- Na analýzu každé navozené situace v rámci inputu je určen časový limit, který moderátor hlídá.
- V některých případech, kdy k tomu dá moderátor svolení, bude možné použít internetu jako zdroje informací.

## 8.2 Odpovědi

- Na každou položenou otázku odpovězte ve stanoveném čase.
- Protože se jedná o týmovou práci, otázky v týmu diskutujte a odpovědi formulujte jako tým společně.
- V případě, že se nemůžete v rámci týmu na výsledné odpovědi shodnout, zaznamenejte to do odpovědního formuláře.

## 8.3 Diskuze

- Mimo diskuze v týmech je možná taktéž diskuze mezi týmy.
- Tuto diskuzi iniciuje a řídí výhradně pouze moderátor (a to i neplánovaně podle průběhu cvičení).

## 8.4 Závěrečný debrief a vyhodnocení

- Po uplynutí stanoveného programu a času bude cvičení ukončeno.
- Moderátor ve spolupráci s hodnotitelem cvičení vyhodnotí.

V dohodnutém termínu bude cvičení za přítomnosti všech týmů shrnuto a účastníci budou seznámeni s výsledky.

# 9 Osnova výuky

Výuka je rozdělena na teoretickou a praktickou část.

## Teoretická část

Před realizací cvičení je nezbytné ujistit se, že témata řešená v praktické části jsou pro žáky známá, pochopená a srozumitelná. Pokud jsou identifikovány oblasti, které nejsou součástí standardního vzdělávání, je nutné je před realizací cvičení probrat. Jedná se o zákonné normy/oblasti, které jsou uvedeny v Použité literatuře a v kontextu k řešeným úkolům v rámci cvičení.

Cvičení se týká smyšleného zdravotnického zařízení v ČR - v organizaci, která poskytuje zdravotní služby v souladu se zákonem č. 372/2011 Sb., zákon o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních

službách).

**Název smyšlené organizace:**

## Zemská nemocnice Priessnitz

**Postavení z pohledu ZoKB:**

- Nemocnice byla v roce 2019 určena NÚKIB jako provozovatel základní služby, a to v souladu se ZoKB.
- Určení proběhlo prostřednictvím správního řízení v souladu se zákonem č. 500/2004 Sb., správní řád.
- Informační systémy nemocnice, na kterých je poskytování této služby závislé, jsou informačními systémy základní služby.
- Určení nemocnice jako provozovatele základní služby, včetně určení informačních systémů základní služby proběhlo v souladu s § 22a ZoKB a vyhláškou č. 437/2017 Sb., o kritériích pro určení provozovatelů základních služeb.
- Počet lůžek: 2300
- Nemocnice poskytuje rovněž vysoce specializovanou traumatologickou péči podle zákona o zdravotních službách.

# Praktická část

## 10 Input 1 - Právní normy

### 10.1 Hierarchie právních norem podle právní síly

Zemská nemocnice Priessnitz je zřízena na území České republiky. Na tomto území existují platné zákonné normy, které jsou součástí běžného života každého státního útvaru.

**10.1.1 Právní normy jsou hierarchicky členěny podle právní síly. Zde uvedené typy právních norem spojte spojnicí od norem s nejvyšší právní sílou po nejnižší s níže umístěnou pyramidou:**

*Čas na zpracování odpovědi: 15‘*

## 10.2 Zákony ČR a právo EU

### 10.2.1 Proč jsou zákony ČR ovlivněny právními akty EU?

*Čas na zpracování odpovědí: 15‘*

ČR je součástí EU.

Ústavní zákon č. 1/1993 Sb., Ústava České republiky

Čl. 1

(2) Česká republika dodržuje závazky, které pro ni vyplývají z mezinárodního práva.

Čl. 10

Vyhlášené mezinárodní smlouvy, k jejichž ratifikaci dal Parlament souhlas a jimiž je Česká republika vázána, jsou součástí právního řádu; stanoví-li mezinárodní smlouva něco jiného než zákon, použije se mezinárodní smlouva.

*Viz hierarchie právních hodnot podle právní síly… 4 – mezinárodní smlouvy a až pod tím 5 – zákony.*

### 10.2.2 Jaké typy EU právních aktů ovlivnily ZoKB, VyKB a OOÚ?

*Čas na zpracování odpovědí: 15‘*

**A. Nařízení** – je od data účinnosti závazné pro členské státy EU.

***Příklad:***

**OOÚ**

GDPR - NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

**KB**

CSA - Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“).

**B. Směrnice** – je transponována do zákonných norem členských států EU.

***Příklad:***

**KB**

NIS1 -> novelizace jak ZoKB, tak i VyKB.

NIS1 - Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.

# 11 Input 2 - Účel a struktura ZoKB a VyKB

## 11.1 Účel a struktura ZoKB

### 11.1.1 Popište účel a strukturu ZoKB

*Čas na zpracování odpovědi: 20‘*

Vzhledem k míře nasazení ICT ve veřejné správě a KII státu a k celosvětovému kontextu (kybernetické hrozby, geopolitická situace) byla ČR nucena definovat zákonný rámec pro oblast KB.

Především se jednalo o zajištění:

- výkonu veřejné moci,
- provozování KII státu.

Viz ZoKB:

§ 1

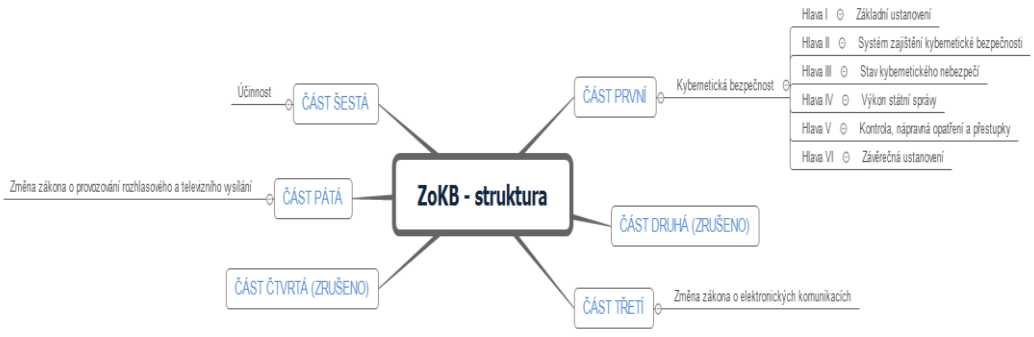
Předmět úpravy

(1) Tento zákon upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti.

(2) Tento zákon zapracovává příslušný předpis Evropské unie[6], zároveň navazuje na přímo použitelný předpis Evropské unie[17] a upravuje zajišťování bezpečnosti sítí elektronických komunikací a informačních systémů.

(3) Tento zákon se nevztahuje na informační nebo komunikační systémy, které nakládají s utajovanými informacemi.

*Poznámky pod čarou:*
[6] – *NIS1*
[17] - CSA



## 11.2 Kybernetický prostor

### 11.2.1 Čím je z pohledu ZoKB tvořen kybernetický prostor (uveďte jeho součásti a paragraf včetně odstavce či písmene)?

*Čas na zpracování odpovědi: 5‘*

Vymezení pojmů

§2, pís a) kybernetickým prostorem digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.

### 11.2.2 Pro kterou ze součástí kybernetického prostoru je určen speciální zákon (uveďte název součásti a číslo a název zákona)?

*Čas na zpracování odpovědi: 5‘*

1. Jedná se o sítě elektronických komunikací.

2. Zákon č. 127/2005 Sb., o elektronických komunikacích.

### 11.2.3 Jaký paragraf a odstavec či písmeno ZoKB definují zajištění bezpečnosti, dostupnosti a spolehlivosti součástí kybernetického prostoru?

*Čas na zpracování odpovědi: 10‘*

Bezpečnostní opatření

§4

(1) Bezpečnostním opatřením se rozumí souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru.

### 11.2.4 Jak jsou dle ZoKB rozdělena bezpečnostní opatření?

*Čas na zpracování odpovědi: 15‘*

*a)* organizační opatření a
*b)* technická opatření.

Vyjmenujte v souladu se ZoKB organizační a technická opatření.

| Organizačními opatřeními jsou | Technickými opatřeními jsou |
|---|---|
| ***a)*** systém řízení bezpečnosti informací,<br>***b)*** řízení rizik,<br>***c)*** bezpečnostní politika,<br>***d)*** organizační bezpečnost,<br>***e)*** stanovení bezpečnostních požadavků pro dodavatele,<br>***f)*** řízení aktiv,<br>***g)*** bezpečnost lidských zdrojů,<br>***h)*** řízení provozu a komunikací,<br>***i)*** řízení přístupu osob,<br>***j)*** akvizice, vývoj a údržba,<br>***k)*** zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,<br>***l)*** řízení kontinuity činností a<br>***m)*** kontrola a audit. | ***a)*** fyzická bezpečnost,<br>***b)*** nástroj pro ochranu integrity komunikačních sítí,<br>***c)*** nástroj pro ověřování identity uživatelů,<br>***d)*** nástroj pro řízení přístupových oprávnění,<br>***e)*** nástroj pro ochranu před škodlivým kódem,<br>***f)*** nástroj pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů,<br>***g)*** nástroj pro detekci kybernetických bezpečnostních událostí,<br>***h)*** nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí,<br>***i)*** aplikační bezpečnost,<br>***j)*** kryptografické prostředky,<br>***k)*** nástroj pro zajišťování úrovně dostupnosti informací a<br>***l)*** bezpečnost průmyslových a řídících systémů. |

### 11.2.5 Jak je dle ZoKB zajištěna bezpečnost informací (uveďte paragraf, odstavec či písmeno)?

*Čas na zpracování odpovědi: 5‘*

Vymezení pojmů

§2

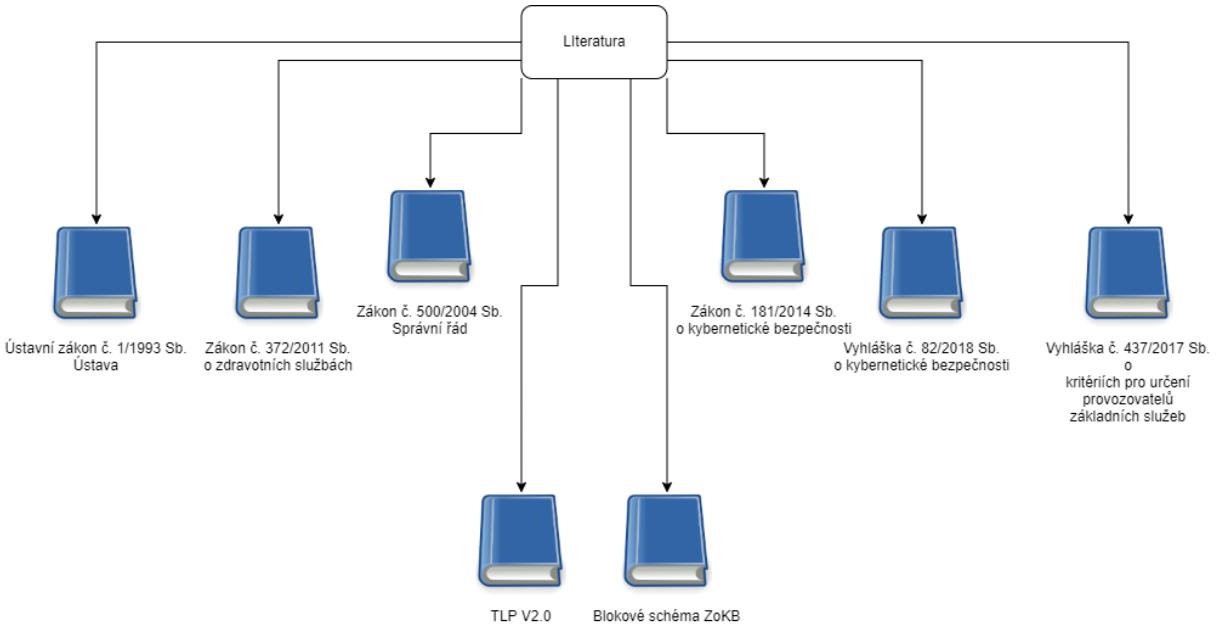
c) bezpečností informací zajištění důvěrnosti, integrity a dostupnosti informací a dat.

# Shrnutí a závěr

Po absolvování tohoto cvičení budou studenti schopni:

- Pochopit důležitost a smysl hierarchie právních norem podle právní síly s vazbou na interní předpisy v jakékoli organizaci.
- Pochopit strukturu právních předpisů.
- Pochopit způsoby aplikace práva EU do legislativy ČR.
- Pochopit smysl aplikace práva pro oblast kybernetického prostoru.
- Pochopit smysl a místo zákona o kybernetické bezpečnosti v našem právním systému.
- Prakticky ověřit, že pro každou právnickou osobu je nezbytné z pohledu jejího fungování zajištění jak provozních/technologických, tak i procesních aspektů s vazbou na lidský faktor, ale taktéž i zajištění bezpečnostní vrstvy ve smyslu zajištění informační a kybernetické bezpečnosti a kontinuity byznysu.

# Seznam použitých zdrojů




**Odkazy na použité zákonné předpisy:**

**Zákonné předpisy**


- Zákony pro lidi

  https://www.zakonyprolidi.cz

- Ústava ČR - ústavní zákon č. 1/1993 Sb.
  https://www.zakonyprolidi.cz/cs/1993-1
- Zákon č. 372/2011 Sb., zákon o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách)
  https://www.zakonyprolidi.cz/cs/2011-372
- Zákon č. 500/2004 Sb., správní řád
  https://www.zakonyprolidi.cz/cs/2004-500
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů
  - https://www.zakonyprolidi.cz/cs/2014-181
  - https://www.zakonyprolidi.cz/cs/2017-205
  - https://www.zakonyprolidi.cz/cs/2022-226
- Zákon č. 205/2017 Sb., zákon, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony
  - https://www.zakonyprolidi.cz/cs/2017-205
- Zákon č. 226/2022 Sb., zákon, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů
  - https://www.zakonyprolidi.cz/cs/2022-226
- Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)
  - https://www.zakonyprolidi.cz/cs/2018-82
- Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatelů základních služeb.

- https://www.zakonyprolidi.cz/cs/2017-437

**Úřad - NÚKIB**

- Web Úřadu - NÚKIB: https://www.nukib.cz/
- Doporučení NÚKIB: https://www.nukib.cz/cs/infoservis/doporuceni/
- TLP: https://www.nukib.cz/cs/infoservis/doporuceni/1862-doporuceni-k-pouzivani-protokolu-tlp-ke-sdileni-chranenych-informaci-2/
- Podpůrné materiály:
  - https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/
  - https://www.nukib.cz/download/publikace/podpurne_materialy/ZKB_blokove_schema.pdf
  - https://www.nukib.cz/download/publikace/podpurne_materialy/Schema_povinnosti.pdf
  - https://www.nukib.cz/download/publikace/podpurne_materialy/Schema_lhuty.pdf
  - https://www.nukib.cz/download/publikace/podpurne_materialy/Schema_rozhodovani_PZS_v2.1.pdf
  - https://www.nukib.cz/download/publikace/podpurne_materialy/Schema_PZS.pdf
  - https://www.nukib.cz/download/publikace/podpurne_materialy/Neprimerene-naklady_v2.1.pdf
- Výkladový slovník kybernetické bezpečnosti: https://www.nukib.cz/download/publikace/podpurne_materialy/vykladovy_slovnik_KB_3_vydani.pdf

**EU**

- **Typy právních aktů EU:** https://ec.europa.eu/info/law/law-making-process/types-eu-law_cs
- CSA: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32019R0881&from=CS
- NIS1: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016L1148&from=cs

**GDPR:**

- https://eur-lex.europa.eu/legal-content/cs/TXT/?uri=CELEX%3A32016R0679

**Použitá literatura:**

ČADOVÁ, Barbara, Jana PETRŽELOVÁ a Miroslava ČERMÁKOVÁ. *Maturitní otázky -občanský a společenskovědní základ*. 1. vyd. Fragment, 2008, 224 s. ISBN 978-80-253-0600-0.

Důvěrnost informací v souladu s TLP 2.0

| Barva | Podmínky použití |
|---|---|
| TLP:RED | Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace. |
| TLP:AMBER | Informace může být sdílena v rámci organizace, které byla informace poskytnuta. Dále může být poskytnuta pouze těm partnerům, kteří splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci. Jiným osobám, než výše uvedeným, nesmí být informace poskytnuta. |
| TLP:AMBER+STRICT | Informace je sdílena pouze s organizací. |
| TLP:GREEN | Informace může být sdílená v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace. |
| TLP:CLEAR | Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena. |

# Příklady použití:

TLP:RED – Od zahraničních partnerů jsme získali informaci, že útočník má přístup do vaší sítě a plánuje spustit ransomware útok. Doporučujeme tedy provést následující protiopatření...

TLP:AMBER – Z našich zjištění vyplývá, že je ve vaší síti používána zranitelná verze firewallu. Doporučujeme co nejdříve provést jeho aktualizaci. Tuto informaci můžete předat správci nebo dodavateli FW.

TLP:AMBER+STRICT – Z našich zjištění vyplývá, že je ve vaší síti používána zranitelná verze firewallu. Doporučujeme co nejdříve provést jeho aktualizaci. Tuto informaci je možné předat pouze v rozsahu vaší organizace.

TLP:GREEN – V České republice nyní probíhá phishing kampaň zaměřující se na zdravotnická zařízení, poučte své uživatele na možná rizika.

TLP:CLEAR – GovCERT.CZ za poslední rok řešil 126 incidentů, z toho 26 závažných.

Pro vice informací o protokolu sledujte oficiální stránky FIRST: https://www.first.org/tlp/