

**OSNOVY MODULU (PŘEDMĚTU) 2**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Kód modulu* |  | | *Název modulu* | **Zákony a předpisy upravující kybernetickou bezpečnost** |
| Fakulta | |  | | |
| Obor studia | |  | | |
| Forma studia | |  | | |
| Úroveň studia | |  | | |
| Profil | |  | | |
| Stav modulu | |  | | |
| Osoba odpovědná za modul | | | |  |
| Osoby vyučující modul | | | |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Forma tříd | Přednášky | Workshopy | | |
| Počet hodin/sem | 6 | 14 | | |
| Semestr(y) |  | | ECTS body |  |
| Stav |  | | Jazyk výuky |  |
| Předpoklady | žádné | | | |

|  |
| --- |
| Cíle učení |
| Cílem modulu je seznámit studenty s aplikací právních institutů v oblasti informačních a komunikačních technologií. Sekundárním cílem je vymezit právní limity kybernetické bezpečnosti.  Po absolvování kurzu by měl student získat schopnost orientovat se v právních normách EU a zemí účastnících se projektu, které přímo souvisejí s problematikou kybernetické bezpečnosti.  Dále student získá základní přehled o problematice občanského a veřejného práva, které se uplatňuje v kyberprostoru, zejména se zaměřením na praktické využití získaných znalostí v praxi. Studenti jsou seznámeni nejen s teorií aplikace práva v kyberprostoru a úpravou de lege lata, ale i s praktickým využitím institutů práva v praxi (de lege aplicata).  Takto získané znalosti budou dále využity v modulech věnovaných kybernetickým útokům a možnostem obrany proti nim a v modulu věnovaném budování a fungování bezpečnostních týmů. |

|  |  |
| --- | --- |
| Výsledek učení | Student, který úspěšně dokončil modul, bude znát/umět/kompetentně ovládat |
| **VĚDOMOSTI** | |
| W1 | Student získá odborné znalosti a rozšíří si právní povědomí v oblasti informačních a komunikačních technologií. |
| W2 | Student získá odborné znalosti týkající se právní definice kybernetické bezpečnosti podle mezinárodního práva (zejména práva EU) a vnitrostátního práva zúčastněných zemí. |
| DOVEDNOSTI | |
| U1 | Je schopen identifikovat jednotlivé poskytovatele internetových služeb, jejich práva a povinnosti a na základě této identifikace je schopen argumentovat v oblastech práva souvisejících s kybernetickou bezpečností. |
| U2 | Je schopen analyzovat základní rámec aktiv v kyberprostoru (např. technologie, procesy, data atd.) a definovat právní doporučení pro jejich ochranu. |
| **SOUTĚŽE** | |
| K1 | Student částečně ovládá právní předpisy, dokáže aplikovat jednotlivé právní instituty na případové studie. |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Metody ověřování výsledků učení** | | | | | | | | | |
| **Výsledek učení** | **Formy kreditních tříd** | | | | | | | | |
| Ústní zkouška | Písemná zkouška | Částečný písemný úkol | Závěrečný písemný úkol (esej atd.) | Test | Projekt/prezentace | Nahlásit | Činnosti ve třídě | Ostatní... |
| VĚDOMOSTI | | | | | | | | | |
| W1 |  | x | x |  | x |  |  | x |  |
| W2 |  | x | x |  | x |  |  | x |  |
| DOVEDNOSTI | | | | | | | | | |
| U1 |  |  |  |  |  | x |  |  |  |
| U2 |  |  |  |  |  | x |  |  |  |
| SOUTĚŽE | | | | | | | | | |
| K1 |  |  | x |  |  |  |  |  |  |

**Kritéria pro hodnocení kompetencí žáka**

**Minimální požadavky na tři skupiny výsledků učení, které musí student získat, aby daný předmět absolvoval, jsou uvedeny níže v syntetické podobě. Aby student mohl modul absolvovat, musí být všechny výsledky učení popsané v sylabu pozitivně ověřeny osobou (osobami), která (které) vede (vedou) výuku v rámci daného modulu**

**W - VĚDOMOSTI**

**Hodnocení:**

**Dostatečné - student si pamatuje a znovu si vybavuje znalosti, které má v rámci modulu zvládnout.**

**Dobrý - Žák dodatečně interpretuje jevy / problémy a dokáže vyřešit typický problém.**

**Velmi dobře -Student dokáže řešit i složité problémy v daném oboru, umí provést syntézu, provést komplexní hodnocení, vytvořit práci, která je originální a inspirativní pro ostatní.**

**U - DOVEDNOSTI**

**Hodnocení:**

**Dostatečný - Student je obeznámen s povahou činností a je schopen pod vedením akademického učitele vykonávat činnosti/řešit problémy související s obsahem modulu.**

**Dobrý - Student je schopen samostatně vykonávat činnosti / úkoly / řešit běžné problémy týkající se obsahu modulu.**

**Velmi dobře - Žák má plně zvládnutou schopnost / dovednost provádět činnosti / úkoly / problémy uvedené v obsahu modulu, a to i ve složitějších případech.**

**K - SOCIÁLNÍ KOMPETENCE**

**Hodnocení:**

**Dostatečný - Student pasivně vstřebává obsah modulu a prokazuje schopnost soustředit se a naslouchat.**

**Dobrý - Žák se aktivně účastní výuky, hodnotí podle kritérií přijatých v daném oboru, dokáže aktivně komunikovat ve skupině.**

**Velmi dobře - Žák integruje postoje podle navrženého vzoru, rozvíjí vlastní systém profesních a společenských hodnot, je schopen převzít odpovědnost za činnost skupiny, včetně vedení.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Obsah modulu (program přednášek a dalších lekcí)** | | **Odkaz na výsledky učení** | |
| PŘEDNÁŠKY  1. Úvod do předmětu, systém práva, právní norma, právo a internet  2. Odpovědnost v kyberprostoru  3. Právní základ činnosti ISP (poskytovatele internetových služeb)  4. ISMS  5. Kybernetická bezpečnost a její právní úprava  6. Ochrana osobních údajů v kyberprostoru  7. Ochrana soukromí a bezpečnost v IKT, ochrana údajů v kyberprostoru  WORKSHOPY   1. Vymezení působnosti práva v kyberprostoru (hranice, možnosti atd.) 2. Soukromoprávní a veřejnoprávní odpovědnost za jednání uživatele nebo společnosti v online prostředí. 3. Charakteristika a definice jednotlivých poskytovatelů internetových služeb a jejich práv a povinností ve vztahu ke kybernetické bezpečnosti 4. ISMS a vztah k zákonu o kybernetické bezpečnosti 5. Získání základních práv a povinností pro jednotlivé subjekty ze směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních pro vysokou společnou úroveň bezpečnosti sítí a informačních systémů v Unii, jakož i z národní legislativy. 6. Uplatňování práv a povinností vyplývajících z GDPR v kyberprostoru 7. Praktická analýza smluvních podmínek s poskytovateli internetových služeb ve vztahu k ochraně soukromí | | W1, W2  U1, U2,  K1 | |
| **Bilance bodů ECTS** | | | |
| Forma pracovního zatížení studentů | | | Počet hodin |
| **Počet hodin realizovaných za přímé účasti akademického pedagoga** | | | |
| 1.1 | Účast na přednáškách | | 6 |
| 1.2 | Účast na seminářích | |  |
| 1.3 | Účast na seminářích | | 14 |
| 1.4 | Účast na laboratorních hodinách | |  |
| 1.5 | Účast na projektech | |  |
| 1.6 | Účast na konzultacích (2-3krát za semestr) | |  |
| 1.7 | Účast na konzultacích k projektu | |  |
| 1.8 | Účast na zkouškách/testech | | 2 |
| 1.9 | Ostatní... | |  |
| **1.10** | **Počet hodin realizovaných za přímé účasti akademického pedagoga (součet 1.1 - 1.9)** | | 22 |
| **1.11** | **Počet ECTS bodů, které student získal v hodinách vyžadujících přímou účast akademického pracovníka)** | | 1,5 |

|  |  |  |
| --- | --- | --- |
| **Individuální práce studenta** | | |
| 2.1 | Individuální studium (včetně e-learningových přednášek) | 8 |
| 2.2 | Individuální příprava na semináře | 12 |
| 2.3 | Individuální příprava na testy |  |
| 2.4 | Individuální příprava na laboratorní výuku |  |
| 2.5 | Příprava zpráv |  |
| 2.6 | Realizace samostatně prováděných úkolů (projekty, dokumentace) |  |
| 2.7 | Příprava na závěrečnou zkoušku/testy ze seminářů | 10 |
| 2.8 | Příprava na závěrečnou zkoušku/testy z přednášek | 15 |
| 2.9 | Další |  |
| **2.10** | **Počet hodin individuální práce (součet 2.1 - 2.9)** | 45 |
| **2.11** | **Počet ECTS bodů, které student získal během individuálních studijních aktivit** | 2,5 |
| **Celková pracovní zátěž (h)** | | **67** |
| **ECTS body za modul** | | **4** |