

ZÁKLADY REGULÁCIE KYBERNETICKEJ BEZPEČNOSTI A SÚVISIACICH OBLASTÍ

Informačný list



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Financované EÚ NextGenerationEU prostredníctvom Plánu obnovy a odolnosti SR v rámci projektu č. 17R05-04-V01-00002.

**Názov a adresa
vzdelávacej inštitúcie:**

Kompetenčné centrum pre reguláciu kybernetickej bezpečnosti, ochrany súkromia a kybernetickej kriminality, Univerzita Komenského v Bratislave, Právnická fakulta, Šafárikovo nám. č. 6, P.O.BOX 313, 810 00 Bratislava (ďalej aj ako „kompetenčné centrum“)

Názov kurzu:

Základy regulácie kybernetickej bezpečnosti a súvisiacich oblastí

Celkový rozsah:

Kurz je poskytovaný v rozsahu 50 vyučovacích hodín. Vyučovací hodina má 45 minút. Kurz sa delí na 5 modulov. Každý modul má 2 časti s časovou dotáciou 5 vyučovacích hodín pre každú časť modulu. Pre pripustenie na záverečné overovanie vedomostí a hodnotenie je potrebné, aby účastník kurzu absolvoval aspoň 80 % výučby (aspoň 4 moduly). Po absolvovaní modulov bude prebiehať záverečné overovanie vedomostí a hodnotenie v trvaní 4 vyučovacích hodín.

Termíny kurzu:

Kurz je poskytovaný v dvoch cykloch. Výučba modulov prebieha piatky podľa harmonogramu od 9:00 do 13:00. Presný harmonogram dostupný na <https://cusec.flaw.uniba.sk/celozivotne-vzdelavanie/zaklady-regulacie-kybernetickej-bezpecnosti-a-suvisiacich-oblasti/>

Organizátor vzdelávania si vyhradzuje právo zmeniť dátumy a čas začiatku jednotlivých modulov.

Forma vzdelávania:

Prednáška, seminár, prípadové štúdie.

Metóda vzdelávania:

Prezenčne v priestoroch kompetenčného centra/v rámci virtuálnej miestnosti (MS TEAMS), kde bude zachovaný reálny čas interakcie a možnosť okamžitých otázok, diskusií a spolupráce medzi účastníkmi.

Cieľová skupina:

Zamestnanec verejnej správy (zamestnanci v štátnej službe, zamestnanci vykonávajúci práce vo verejnom záujme alebo v služobnom pomere) v kategórii používateľa - laik, odborný zamestnanec a manažér v zmysle vyhlášky Národného bezpečnostného úradu č. 492/2022 Z. z., ktorou sa ustanovujú znalostné štandardy v oblasti kybernetickej bezpečnosti.

Laik - používateľ IKT okrem výkonu konkrétneho povolania.

Odborný zamestnanec - používateľ, ktorý pri výkone povolania využíva sieť alebo informačný systém.

Manažér - riadiaci zamestnanec, ktorý nie je IT manažérom alebo manažérom kybernetickej bezpečnosti a ktorý spravidla zodpovedá za príslušný proces alebo skupinu procesov a v rámci nich zodpovedá aj za plnenie úloh v oblasti riadenia rizík kybernetickej bezpečnosti.

Profil absolventa:

Absolvent kurzu celoživotného vzdelávania „Základy regulácie kybernetickej bezpečnosti a súvisiacich oblastí“ disponuje pevnými základmi právnej a regulačnej problematiky v oblasti kybernetickej bezpečnosti. Získal komplexný prehľad o právnych, technických aj strategických aspektoch regulácie, a to v kontexte právneho poriadku Slovenskej republiky, ako aj práva Európskej únie.

Počas štúdia absolvoval úvod do problematiky regulácie kybernetickej bezpečnosti, kde sa oboznámil s hlavnými princípmi právnej úpravy, aplikačnými problémami a dopadmi na ľudské práva. Zvládol základné právne rámce vrátane smernice NIS 2, Aktu o kybernetickej bezpečnosti, Aktu o kybernetickej odolnosti, ako aj národnej legislatívy, najmä zákona o kybernetickej bezpečnosti a zákona o informačných technológiách verejnej správy.

Absolvent má prehľad o regulácii ochrany súkromia a osobných údajov, vrátane právnych inštitútov podľa GDPR, pôsobnosti dozorných orgánov a o prepojení ochrany údajov s kybernetickou bezpečnosťou. Rovnako rozumie základom regulácie kybernetickej kriminality – od skutkových podstát trestných činov, cez nástroje získavania a uchovávanía digitálnych dôkazov, až po mechanizmy medzinárodnej justičnej spolupráce.

Kurz mu zároveň umožnil získať orientáciu v širších súvislostiach digitálnej regulácie EÚ, vrátane strategických dokumentov a nových výziev ako sú hybridné hrozby, dezinformácie, umelej inteligencie či digitálne platformy, regulované prostredníctvom aktu o umelej inteligencii a aktu o digitálnych službách.

Vďaka nadobudnutým vedomostiam je absolvent pripravený uplatniť sa v súkromnom aj verejnom sektore, najmä v oblastiach compliance, právneho poradenstva, tvorby interných politík kybernetickej bezpečnosti či v oblasti ochrany osobných údajov a prevencie kybernetických hrozieb.

Lektori:

doc. JUDr. Jozef Andraško, PhD., Mgr. Petra Dražová, PhD., JUDr. Zoltán Gyurász, PhD., JUDr. Matúš Mesarčík, PhD., LL.M., doc. JUDr. Marek Kordík, PhD., LL.M., prof. JUDr. Jozef Čentéš, DrSc.; JUDr. Lukáš Turay, PhD.

Podmienky na absolvovanie kurzu:

Záverečné overovanie vedomostí a hodnotenie. Získanie minimálne 60% hodnotenia.

Vyučovací jazyk:

slovenský jazyk

Doklad o absolvovaní kurzu:

osvedčenie o absolvovaní kurzu

Predmetný kurz sa skladá z nasledujúcich modulov:

MODUL 1 „Úvod do regulácie kybernetickej bezpečnosti“

Modul 1 sa zameriava na vysvetlenie problematiky regulácie kybernetickej bezpečnosti s poukázaním na aplikačné problémy. Predmetom vzdelávania budú témy ako regulačné nástroje kybernetickej bezpečnosti, princípy právnej úpravy kybernetickej bezpečnosti, teoreticko-technické východiská kybernetickej bezpečnosti, vplyv kybernetickej bezpečnosti na ľudské práva, regulácia z pohľadu práva EÚ a právneho poriadku Slovenskej republiky.

Stručná osnova:

- regulačné nástroje kybernetickej bezpečnosti,
- princípy právnej úpravy kybernetickej bezpečnosti,
- teoreticko-technické východiská kybernetickej bezpečnosti,
- kybernetická bezpečnosť ako prax a ako stav,
- vplyv kybernetickej bezpečnosti na ľudské práva.

MODUL 2 „Základy právnej úpravy kybernetickej bezpečnosti“

Modul 2 sa zameriava na základnú charakteristiku relevantnej právnej úpravy kybernetickej bezpečnosti v Európskej únii a Slovenskej republike. Predmetom vzdelávania budú regulačné aspekty smernice NIS 2, Akt o kybernetickej bezpečnosti a Akt o kybernetickej odolnosti. Slovenské právne prostredie budú reprezentovať témy týkajúce sa zákona o kybernetickej bezpečnosti a zákona o informačných technológiách verejnej správy, ich vzájomných súvislostí a presahu na európsku právnu úpravu.

Stručná osnova:

- základy regulácie kybernetickej bezpečnosti na úrovni práva Európskej únie,
- právo Európskej únie - smernica NIS 2,
- právo Európskej únie - Akt o kybernetickej bezpečnosti,
- právo Európskej únie - Akt o kybernetickej odolnosti,
- zákon o kybernetickej bezpečnosti a príslušné vyhlášky,
- zákon o informačných technológiách vo verejnej správe a príslušná vyhláška.

MODUL 3 „Základy regulácie ochrany súkromia a ochrany osobných údajov“

Modul 3 sa zameria na vysvetlenie problematiky regulácie ochrany súkromia a osobných údajov s poukázaním na aplikačné problémy. Predmetom vzdelávania budú témy, ktoré sa týkajú práva na súkromie a práva na ochranu osobných údajov, podrobné vysvetlenie pôsobnosti, základných pojmov, jednotlivých inštitútov a dozoru podľa GDPR, prekrývanie s oblasťou kybernetickej bezpečnosti. Zároveň budú predmetom výkladu aj súvisiace právne rámce ochrany údajov v EÚ.

Stručná osnova:

- právo na súkromie a právo na ochranu osobných údajov, dilema ochrany súkromia verzus bezpečnosť,
- legislatíva ochrany osobných údajov v Európskej únii a Slovenskej republike - stručný úvod,
- všeobecné nariadenie o ochrane osobných údajov - úvod, základná orientácia, pôsobnosť,
- všeobecné nariadenie o ochrane osobných údajov - základné zásady spracúvania, bezpečnosť a zodpovednosť pri spracúvaní osobných údajov,
- všeobecné nariadenie o ochrane osobných údajov - cezhraničné prenosy, dozorné orgány a ich činnosť.

MODUL 4 „Základy regulácie kybernetickej kriminality“

Modul 4 sa zameriava na hmotnoprávnu analýzu skutkových podstát kybernetických trestných činov, medzinárodných prameňov a európskej legislatívy. Druhá časť kurzu poskytne účastníkovi prehľad a výklad nástrojov získavania a zabezpečovania digitálnych stôp, tak aby tieto mohli byť použiteľné ako

elektronické dôkazy v trestnom konaní, vrátane nástrojov justičnej spolupráce v trestných veciach a relevantných medzinárodných dohovorov v tejto oblasti.

Stručná osnova:

- fyzická a právnická osoba ako páchatel' a poškodený kybernetickou kriminalitou,
- hmotnoprávna analýza skutkových podstat kybernetických trestných činov,
- zaistovanie digitálnych stôp v SR,
- zaistovanie digitálnych stôp v EU kontexte,
- zaistovanie digitálnych stôp v medzinárodnom kontexte.

MODUL 5 „Širšie regulačné súvislosti kybernetickej bezpečnosti v kontexte digitálnych politík Európskej únie“

Modul sa zameriava na širšie súvislosti regulácie kybernetickej bezpečnosti v kontexte digitálnych politík Európskej únie. Modul poslucháčom predstaví základné strategické dokumenty na úrovni Európskej únie a zameria sa na reguláciu najnovších trendov súvisiacich s kybernetickou bezpečnosťou ako umelá inteligencia (Akt o umelej inteligencii), hybridné hrozby, dezinformácie a sociálne média (Akt o digitálnych službách).

Stručná osnova:

- Úvod do politík jednotného digitálneho trhu EÚ - základné princípy a prehľad legislatívy, kontext kybernetickej bezpečnosti,
- Akt o umelej inteligencii - úvod, základný prehľad, klasifikácia systémov AI, požiadavky na kybernetickú bezpečnosť,
- Akt o digitálnych službách - úvod, základný prehľad, klasifikácia digitálnych služieb, kontext kybernetickej bezpečnosti,
- Hybridné hrozby a dezinformácie - prehľad právnych nástrojov boja proti dezinformáciám v online priestore.