ZODPOVEDNOSTNÉ VZŤAHY V KYBERNETICKEJ BEZPEČNOSTI

Informačný list

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:	Zodpovednostné vzťahy v kybernetickej bezpečnosti
Celkový rozsah:	Kurz je poskytovaný v rozsahu 50 vyučovacích hodín. Vyučovacia hodina má 45 minút. Kurz sa delí na 5 modulov. Každý modul má 2 časti s časovou dotáciu 5 vyučovacích hodín pre každú časť modulu. Pre pripustenie na záverečné overovanie vedomostí a hodnotenie je potrebné, aby účastník kurzu absolvoval aspoň 70 % výučby (aspoň 7 stretnutí). Po absolvovaní modulov bude prebiehať záverečné overovanie vedomostí a hodnotenie v trvaní 4 vyučovacích hodín.
Termíny kurzu:	Výučba modulov prebieha piatky podľa harmonogramu od 9:00 do 13:00. Harmonogram: 9.1.2026 16.1.2026 23.1.2026 30.1.2026 6.2.2026 13.2.2026 20.2.2026 27.2.2026 6.3.2026 13.3.2026 Organizátor vzdelávania si vyhradzuje právo zmeniť dátumy a čas začiatku jednotlivých modulov.
Kapacita:	120 účastníkov.
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 - IT manažér, informatik, zamestnanec v kybernetickej bezpečnosti v zmysle vyhlášky Národného bezpečnostného úradu č. 492/2022 Z. z., ktorou sa ustanovujú znalostné štandardy v oblasti kybernetickej bezpečnosti.

IT manažér - riadiaci zamestnanec organizačných jednotiek zodpovedných za poskytovanie IT služieb, návrh, implementáciu, obstaranie, prevádzku, údržbu a posudzovanie prostriedkov IKT.

Informatik - zamestnanec zodpovedný za poskytovanie IT služieb, návrh, implementáciu, obstaranie, prevádzku, údržbu a posudzovanie IKT.

Zamestnanec v kybernetickej bezpečnosti - zamestnanec špecializovaný na oblasť bezpečnosti informácií a riadenia rizík kybernetickej bezpečnosti, zodpovedný za návrh, implementáciu, obstaranie, prevádzku, údržbu a posudzovanie bezpečnostných mechanizmov a riešení.

Profil absolventa:

Absolvent kurzu „Zodpovednostné vzťahy v kybernetickej bezpečnosti" disponuje uceleným právnym, regulačným a technickým prehľadom o zodpovednostných vzťahoch v oblasti kybernetickej bezpečnosti na národnej aj európskej úrovni. V rámci kurzu získal vedomosti o všeobecných právnych základoch kybernetickej bezpečnosti, o prepojení tejto oblasti s inými právnymi disciplínami a o uplatňovaní technických noriem v praxi.

Absolvent rozumie zodpovednosti regulovaných subjektov, najmä v kontexte implementácie bezpečnostných opatrení, riadenia zmluvných vzťahov v dodávateľskom reťazci, správy zraniteľností a reakcie na bezpečnostné incidenty. Vie analyzovať a rozlišovať medzi súkromnoprávnou a verejnoprávnou zodpovednosťou, a je oboznámený aj s možnosťami poistenia kybernetických rizík.

Osvojil si poznatky o špecifikách právnej zodpovednosti v kľúčových sektoroch ako sú informačné systémy verejnej správy, kritická infraštruktúra, OT/ICS systémy, finančný a telekomunikačný sektor, ochrana osobných údajov, umelá inteligencia a ESG. V týchto oblastiach vie identifikovať osobitné právne a regulačné požiadavky v súvislosti s kybernetickou bezpečnosťou.

Absolvent má taktiež prehľad o zodpovednostných vzťahoch osôb v rámci vybraných bezpečnostných rolí definovaných v právnych predpisoch, najmä s ohľadom na znalostné štandardy pre špecialistov a manažérov kybernetickej bezpečnosti. Vie posúdiť zodpovednosť týchto osôb pri výkone operatívnych a riadiacich bezpečnostných činností vrátane dodržiavania požiadaviek na súlad.

V neposlednom rade rozumie problematike kybernetickej kriminality a právnym aspektom zaisťovania digitálnych stôp, vrátane trestnoprávnej zodpovednosti fyzických aj právnických osôb. Ovláda princípy compliance, postupy pri odstraňovaní nezákonného obsahu a vie navrhovať

	preventívne opatrenia proti porušeniu zákona v digitálnom priestore. Vďaka multidisciplinárnemu prístupu je absolvent pripravený čeliť výzvam kybernetickej bezpečnosti v právnej, technickej aj organizačnej rovine a efektívne prispievať k riadeniu kybernetických rizík v rôznych typoch organizácií.
Lektori:	doc. JUDr. Jozef Andraško, PhD., JUDr. Michal Rampášek., Mgr. Petra Dražová, PhD., doc. JUDr. Marek Kordík, PhD., LL.M., JUDr. Lukáš Turay, PhD., Mgr. Roland Hochmann, prof. JUDr. Jozef Čentéš, DrSc., JUDr. Laura Fotopulosová, 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: „Všeobecná časť"
Modul 1 sa zameriava na úvod do zodpovednostných vzťahov v kybernetickej bezpečnosti, ktoré budú bližšie rozobrané v ďalších moduloch, zahŕňajúc európsku a národnú právnu úpravu, vzťahy medzi kybernetickou bezpečnosťou a inými oblasťami práva, a technické normy. Okrem toho sa modul venuje právnej zodpovednosti, identifikácii zodpovedných subjektov a analýze zodpovednostných vzťahov na národnej a európskej úrovni v oblasti kybernetickej bezpečnosti.

Stručná osnova:
- koncept zodpovednosti so zameraním na pojem právnej zodpovednosti,
- vymedzenie základných druhov právnej zodpovednosti, ich členenie a rozdiely medzi nimi,
- základné princípy súkromnoprávnej zodpovednosti,
- základné princípy verejnoprávnej zodpovednosti vo vzťahu ku kybernetickej bezpečnosti,
- administratívnoprávna trestnoprávna zodpovednosť (spoločné a rozdielne znaky),
- základy administratívnoprávnej zodpovednosti v oblasti kybernetickej bezpečnosti.

MODUL 2: „Zodpovednosť regulovaných subjektov"
Modul 2 sa zaoberá zodpovednosťou regulovaných subjektov v oblasti kybernetickej bezpečnosti, vrátane implementácie bezpečnostných opatrení a riadenia zmluvných vzťahov v rámci dodávateľského reťazca. Taktiež pokrýva postupy pri bezpečnostných incidentoch, správu a oznamovanie zraniteľností, a analyzuje súkromnoprávnu a verejnoprávnu zodpovednosť, ako aj možnosti poistenia kybernetických rizík.

Stručná osnova:
- právny rámec kybernetickej bezpečnosti v EÚ a SR,
- vzťah medzi reguláciou a technickými normami,
- zodpovednosť subjektov a tretích strán,
- bezpečnostné opatrenia a riadenie rizík,
- riadenie incidentov a hlásenie udalostí,
- dohľad, audit a poistenie.

MODUL 3: „Zodpovednosť v osobitných oblastiach"
Modul 3 sa sústreďuje na zodpovednosť v špecifických oblastiach kybernetickej bezpečnosti, zahŕňajúc ITVS/ISVS, kritickú infraštruktúru, OT/ICS, finančný sektor, telekomunikácie, ochranu osobných údajov, umelú inteligenciu a ESG. Tento modul poskytuje náhľad do právnych a regulačných požiadaviek týkajúcich sa kybernetickej bezpečnosti v kritických oblastiach a súvisiacich prepojených oblastiach.

Stručná osnova:

- špecifiká zodpovednosti v oblasti ISVS/ITVS a verejného sektora,
- kybernetická bezpečnosť v kritickej infraštruktúre a OT systémoch,
- ochrana osobných údajov a kybernetická bezpečnosť,
- kybernetická bezpečnosť vo finančnom sektore,
- umelá inteligencia a kybernetická bezpečnosť,
- ESG a kybernetická bezpečnosť.

MODUL 4: „Zodpovednostné vzťahy osôb pre vybrané bezpečnostné role"
Modul 4 skúma zodpovednostné vzťahy osôb pre vybrané bezpečnostné role, pričom vychádza z požiadaviek na znalostné štandardy v oblasti kybernetickej bezpečnosti pre rôzne role, ako sú špecialista a manažér kybernetickej bezpečnosti podľa vyhlášky č. 492/2022 Z. z. Zameriava sa na riadenie bezpečnosti, hrozieb a rizík, aplikáciu bezpečnostných opatrení, výkon operatívnych bezpečnostných činností, riadenie súladu a posudzuje súkromnoprávnu a verejnoprávnu zodpovednosť.

Stručná osnova:

- prehľad bezpečnostných rolí podľa ENISA CSF a vyhlášky NBÚ č. 492/2022 Z. z.,
- rozdelenie zodpovednosti v jednotlivých bezpečnostných roliach,
- trestnoprávna a administratívna zodpovednosť v kontexte jednotlivých bezpečnostných rolí,
- civilná zodpovednosť v pracovných a dodávateľských vzťahoch,
- praktické modelové situácie a analýza judikatúry.

MODUL 5: „Kybernetická kriminalita a zaisťovanie digitálnych stôp"
Modul 5 sa zameriava na kybernetickú kriminalitu a právne aspekty zaisťovania digitálnych stôp, vrátane trestnoprávnej zodpovednosti nielen fyzických osôb ale aj právnických osôb a dodržiavania postupov súladu a prevencie (Compliance). Rovnako pokrýva postupy na odstraňovanie nezákonného obsahu, čím poskytuje komplexný prehľad o právnych a operatívnych opatreniach v oblasti kybernetickej bezpečnosti.

Stručná osnova:

- trestné činy na úseku kybernetickej kriminality,
- trestná zodpovednosť fyzických osôb a právnických osôb, Compliance,
- zaisťovanie digitálnych stôp na diaľku a in natura v národnom, európskom a medzinárodnom kontexte,
- zaisťovanie obsahu komunikácie a biometrických údajov v národnom, európskom a medzinárodnom kontexte,
- odstraňovanie nezákonného obsahu v trestnom konaní a mimo trestného konania.