Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Metodika k výučbe predmetu - Právo kybernetickej bezpečnosti a kyberkriminality

v rámci magisterského študijného programu Aplikovaná informatika

(aktivita A2 - Tvorba metodík a vzdelávacích materiálov pre účely vzdelávania v oblasti kybernetickej a informačnej bezpečnosti)

Košice, marec 2026

Názov predmetu: Právo kybernetickej bezpečnosti a kyberkriminality
Kód predmetu: KOPaHP/PKBaK/25

Krátka anotácia predmetu:

Predmet poskytuje komplexný pohľad na kybernetickú bezpečnosť z právneho hľadiska. Zameriava sa na pochopenie základných princípov ochrany informačných systémov, kybernetických hrozieb a bezpečnostných incidentov, ako aj na právny rámec ich regulácie na úrovni Európskej únie a Slovenskej republiky. Študenti sa oboznámia s fungovaním subjektov v oblasti kybernetickej bezpečnosti vrátane jednotiek CSIRT, s implementáciou bezpečnostných opatrení ako aj s rôznymi právnymi inštitútmi (napr. riešenie a hlásenie kybernetických bezpečnostných incidentov, blokovanie škodlivej aktivity). Súčasne sa predmet zameriava na špecifickú skupinu trestnej činnosti, a to na kybernetickú kriminalitu. Študenti majú možnosť sa oboznámiť s hmotnoprávnymi a procesnoprávnymi aspektami tejto problematiky, najmä s konkrétnymi trestnými činmi a spôsobmi ich vyšetrovania.

Cieľová skupina:

Študenti magisterského štúdia programov aplikovanej informatiky a práva (AIm, PM2d).

Ciele vzdelávania

Predmet sprostredkuje študentom poznatky z oblasti problematiky práva kybernetickej bezpečnosti a vyšetrovania kyberkriminality. Študent nadobudne poznatky aj z ďalších oblastí súvisiacich s témou riešenia kybernetických bezpečnostných incidentov, bezpečnostných zraniteľností ako aj zaisťovania digitálnych stôp.

Stručná osnova predmetu:

1) Úvod do práva kybernetickej bezpečnosti, základné princípy, kyberpriestor.
2) Technické aspekty kybernetickej bezpečnosti, model informačnej bezpečnosti.
3) Základy právnej úpravy kybernetickej bezpečnosti na úrovni Európskej únie a v Slovenskej republike.
4) Subjekty v oblasti kybernetickej bezpečnosti, ich postavenie. Koncept bezpečnostných opatrení.
5) Kybernetické bezpečnostné incidenty, ich hlásenie a riešenie.
6) Blokovanie v oblasti kybernetickej bezpečnosti. Bezpečnostné zraniteľnosti, ich životný cyklus a koordinované zverejňovanie zraniteľností.
7) Kybernetická bezpečnosť v kontexte iných právnych rámcov (ochrana osobných údajov, elektronické komunikácie, finančné služby).
8) Kybernetická bezpečnosť vo verejnej správe.
9) Technická normalizácia a certifikácia v kybernetickej bezpečnosti.
10) Úvod do kybernetickej kriminality.
11) Vybrané trestné činy kybernetickej kriminality.

12) Úvod do vyšetrovania kybernetickej kriminality.
13) Zaisťovanie digitálnych stôp a elektronické dôkazy.

Odporúčaná literatúra:

- Andraško, J., Mesarčík, M., Sokol, P.: Právo kybernetickej bezpečnosti. 1. vyd. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2022.
- Smejkal, V. et al.: Právo informačních a telekomunikačních systémů. 2. aktualizované a rozšířené vydání. Praha : C.H.Beck, 2004.
- Polčák, R. et al.: Právo informačních technologií. Praha: Wolters Kluwer ČR, 2018.
- Ivor, J., Polák, P., Záhora, J.: Trestné právo procesné I. Bratislava: Wolters Kluwer, 2021.

Vyučujúci:

- doc. JUDr. Regina Hučková, PhD.
- doc. JUDr. Diana Treščáková, PhD.
- doc. RNDr. JUDr. Pavol Sokol, PhD. et PhD.
- JUDr. Laura Bachňáková Rózenfeldová, PhD.
- prof. JUDr. Sergej Romža, PhD.

Detailná osnova predmetu

Téma 1: Úvod do kybernetickej bezpečnosti

Obsah: Základné pojmy, princípy a modely kybernetickej a informačnej bezpečnosti. Prepojenie ľudí, procesov a technológií.

Podtémy:

- CIA triáda (dôvernosť, integrita, dostupnosť),
- kybernetická bezpečnosť ako proces (ľudia – procesy – technológie),
- kybernetické hrozby,
- úvod do riadenia bezpečnosti (PDCA, ISMS).

Metódy: prednáška, prípadová štúdia, diskusia.

Téma 2: Právna úprava kybernetickej bezpečnosti

Obsah: Právny rámec na úrovni Európskej únie a Slovenskej Republiky. Základné princípy právnej regulácie.

Podtémy:

- Európska právna úprava – NIS, NIS2, GDPR, CRA,
- Slovenská právna úprava - ZoKB a ZoITVS,
- princípy regulácie (technologická neutralita, ochrana údajov, risk-based).

Metódy: prednáška, práca s legislatívou, diskusia.

Téma 3: Subjekty a sektory kybernetickej bezpečnosti

Obsah: Inštitucionálne zabezpečenie kybernetickej bezpečnosti. Vysvetlenie sektorov kybernetickej bezpečnosti.

Podtémy:

- postavenie ústredných orgánov,
- postavenie Národného bezpečnostného úradu,
- jednotky CSIRT (SK-CERT, CSRT.SK),
- prevádzkovatelia (kritických) základných služieb,
- manažér kybernetickej bezpečnosti.

Metódy: prednáška, práca s legislatívou, diskusia.

Téma 4: Zmluvné aspekty kybernetickej bezpečnosti

Obsah: Právne vzťahy a outsourcing služieb v oblasti kybernetickej bezpečnosti.

Podtémy:

- zmluvné aspekty kybernetickej bezpečnosti,
- predmet zmlúv uzatváraných v oblasti kybernetickej bezpečnosti,
- zmluva o úrovni poskytovaných služieb (SLA),
- ochrana informácia vrátane NDA,
- zmluvná ochrana informácií,
- zodpovednostné aspekty.

Metódy: prednáška s diskusiou, prípadové štúdie

Téma 5: Blokovanie a zásahy do práv

Obsah: Blokovanie obsahu a jeho právne implikácie.

Podtémy:

- typy blokovania (statické, dynamické).
- techniky blokovania,
- Zásah do základných práv,

- princíp proporcionality,
- prípady blokovania vo vnútroštátnom rámci.

Metódy: prednáška s diskusiou, prípadové štúdie

Téma 6: Bezpečnostné incidenty a zraniteľnosti

Obsah: Definícia kybernetického bezpečnostného incidentu vrátane jeho riešenia a hlásenia. Definícia bezpečnostnej zraniteľnosti vrátane jej životného cyklu a hlásenia/zverejnenia.

Podtémy:

- bezpečnostný incident vs. udalosť,
- riešenie kybernetických bezpečnostných incidentov (detekcia, reakcia, obnova),
- hlásenie kybernetických bezpečnostných incidentov,
- definícia bezpečnostnej zraniteľnosti,
- životný cyklus bezpečnostnej zraniteľnosti,
- koordinované zverejňovanie zraniteľností.

Metódy: interaktívna prednáška, prípadová štúdia reálneho kybernetického bezpečnostného incidentu a zraniteľnosti

Téma 7: Kybernetická bezpečnosť v kontexte iných regulácií

Obsah: Vzťah právnej úpravy kybernetickej bezpečnosti k súvisiacim právnym úpravám (ochrana osobných údajov, elektronické komunikácie, platobné služby, elektronické služby).

Podtémy:

- kybernetická bezpečnosť v kontexte iných regulácií –všeobecne,
- ochrana osobných údajov,
- ochrana súkromia v elektronických komunikáciách,
- regulácia platobných služieb vo finančnom sektore,
- elektronické služby verejnej správy a elektronické podpisovanie.

Metódy: prednáška, prípadová štúdia, diskusia.

Téma 8: Kybernetická bezpečnosť vo verejnej správe

Obsah: Právna úprava kybernetickej a informačnej bezpečnosti vo verejnej správe. Špecifiká právnych subjektov, riešenia kybernetických bezpečnostných incidentov, bezpečnostných opatrení a bezpečnostných zraniteľností.

Podtémy:

- sektory verejnej správy,

- informačný systém verejnej správy vs. informačná technológia verejnej správy (ďalej len „ITVS“),
- subjekty kybernetickej a informačnej bezpečnosti vo verejnej správe – orgán vedenia, riadenia, správca a prevádzkovateľ ITVS,
- riadenie bezpečnosti ITVS,
- bezpečnostné opatrenia vo verejnej správe,
- riešenie kybernetických bezpečnostných incidentov,
- riešenie bezpečnostných zraniteľností.

Metódy: prednáška, prípadová štúdia, diskusia.

Téma 9: Normalizácia a certifikácia

Obsah: Technická normalizácia predstavuje kľúčový nástroj na zabezpečenie kvality, interoperability a bezpečnosti v oblasti kybernetickej bezpečnosti.

Podtémy:

- technická norma,
- právny rámec technickej normalizácie na úrovni EÚ.
- právny rámec technickej normalizácie na národnej úrovní,
- národné a medzinárodné organizácie,
- harmonizované normy a ich význam pri preukazovaní zhody s právnymi požiadavkami,
- certifikácia kybernetickej bezpečnosti,
- EUCC schéma.

Metódy: prednáška, prípadová štúdia, diskusia.

Téma 10: Kybernetická kriminalita

Obsah: Základné formy kybernetickej kriminality a ich právna kvalifikácia.

Podtémy:

- úvod do kybernetickej kriminality,
- Dohovor o počítačovej kriminalite,
- právna úprava kybernetickej kriminality v EÚ,
- vnútroštátna právna úprava kybernetickej kriminality,
- analýza vybraných trestných činov.

Metódy: prednáška, prípadová štúdia, diskusia.

Téma 11–12: Vyšetrovanie kybernetickej kriminality

Obsah: Zaisťovanie dôkazov a vyšetrovanie.

Podtémy:

- trestné konanie,
- dokazovanie v trestnom konaní,
- dôkaz vs. dôkazný prostriedok,
- digitálne/elektronické stopy,
- zaisťovanie elektronických stôp,
- digitálna forenzná analýza,
- princípy a fázy digitálnej forenznej analýzy,
- súdnoznalecká činnosť.

Metódy: prednáška, prípadová štúdia, diskusia.

Podmienky hodnotenia

Forma ukončenia: klasifikované hodnotenie.

Záverečné hodnotenie z predmetu bude prebiehať formou písomného spracovania zadania obsahovo zameraného na právne riešenie konkrétnych problémov.

Pri hodnotení sa bude vychádzať z nasledovných kritérií: (1.) metodologická, metodická stránka; (2.) preukázanie teoretických vedomostí o spracovanej téme a analytická činnosť; (3.) práca s literatúrou a inými informačnými zdrojmi, formálna úprava; (4.) obhajoba semestrálnej práce: prezentácia, diskusia, odpovede na otázky.

Ak na základe vyhodnotenia vypracovaného zadania nebude študent úspešný, má právo na

vypracovanie opravného zadania v stanovenom termíne.

Stupnica hodnotenia:

- A (30–27 bodov)
- B (26–24 bodov)
- C (23–21 bodov)
- D (20–19 bodov)
- E (18–17 bodov)
- Fx (16 – 0 bodov)

Študent vypracuje právnu analýzu (case study) a musí sa vyjadriť k týmto okruhom:

1. Všeobecný popis organizácie (6b) - Analyzujte právne postavenie organizácie, jej zaradenie podľa relevantnej právnej úpravy kybernetickej bezpečnosti a identifikujte jej kľúčové informačné systémy, aktíva a hrozby.

2. Kybernetický bezpečnostný incident (6b) - Posúďte charakter incidentu, jeho právnu kvalifikáciu, ohlasovacie povinnosti a povinnosti organizácie pri jeho riešení.

3. Plnenie bezpečnostných opatrení (6b) - Zhodnoťte, aké bezpečnostné opatrenia má organizácia implementovať a ktoré z nich by pomohli predísť incidentu alebo zmierniť jeho dopady.

4. Zmluva o poskytovaní služieb v oblasti kybernetickej bezpečnosti (6b) - Navrhnite rámcovú zmluvu s externým dodávateľom pokrývajúcu riešenie incidentov a správu zraniteľností vrátane základných zmluvných náležitostí.

5. Kybernetická kriminalita (6b) - Kvalifikujte skutok z pohľadu trestného práva, identifikujte relevantné trestné činy a určte možné trestné sadzby a okolnosti ovplyvňujúce trest.

Spôsob obhajoby: prezentácia hlavných záverov, diskusia a odpovede na otázky.