Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Metodika pre lektora

Vzdelávanie pre zamestnancov verejnej správy v kategórii používateľov „laik“, „odborný zamestnanec“ a „manažér“

verzia 2.0

Košice, marec 2026

Úvodné poznámky

Krátka anotácia vzdelávania

Vzdelávací program pre zamestnancov verejnej správy v kategórií používateľov „laik“, „odborný zamestnanec“ a „manažér“ sa zameriava na posilnenie bezpečnostného povedomia, zvyšovanie vedomostí a zručností v oblasti kybernetickej a informačnej bezpečnosti (KIB). Cieľom vzdelávania je zvýšiť úroveň bezpečného správania sa používateľov v digitálnom prostredí, a tým prispieť k celkovému znižovaniu bezpečnostných rizík v organizáciách ako aj v online priestore. Program je rozdelený do tematických modulov, ktoré kombinujú teoretické poznatky s praktickými úlohami. Účastníci sa oboznámia so základnými pojmami KIB, významom bezpečnosti z pohľadu jednotlivca aj organizácie, ako aj s aktuálnymi hrozbami podľa analýz ENISA Threat Landscape. V rámci praktických činností sa budú venovať identifikácii aktív, hrozieb, zraniteľností a rizík vo vlastnom prostredí. Samostatné moduly sú venované kritickému mysleniu a dezinformáciám ako aj sociálnemu inžinierstvu - významnej bezpečnostnej hrozbe zameranej na manipuláciu používateľov. Účastníci sa naučia rozpoznávať formy útokov, hoaxy a dezinformácie, precvičia si kritické myslenie a absolvujú phishingový test. Dôležitou súčasťou vzdelávania je aj problematika bezpečnej práce s informačnými a komunikačnými technológiami, a to najmä pri manipulácii s citlivými údajmi a rozpoznávaní škodlivého kódu. Účastníci sa naučia nastavovať základné bezpečnostné prvky mobilných zariadení a oboznámia sa s princípmi riešenia bezpečnostných incidentov z pohľadu bežného používateľa. Osobitný dôraz je kladený na tému digitálnej identity a identifikácie používateľov. Vysvetlené budú princípy tvorby silných hesiel, význam viacfaktorového overovania a používanie správcu hesiel. Modul zároveň upozorní na špecifiká rizík v online prostredí a ukáže, ako ich efektívne zvládať pomocou dostupných nástrojov a bezpečnostných opatrení. Súčasťou vzdelávacieho programu je aj zvyšovanie právneho povedomia v oblastiach práva informačných a komunikačných technológií, ktoré sú úzko prepojené s KIB. Moduly sa bližšie venujú témam ako ochrana osobných údajov, duševné vlastníctvo, právna zodpovednosť v online priestore, elektronická identifikácia, elektronický podpis a kybernetická kriminalita.

Cieľová skupina

Cieľovou skupinou sú kategórie používateľov „laik“, „odborný zamestnanec“ a „manažér“. V zmysle prílohy č. 1 vyhlášky NBÚ 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.

Ciele vzdelávania

Absolventi vzdelávacieho programu budú schopní:

Laik:

- porozumieť vybraným základným pojmom kybernetickej bezpečnosti,
- porozumieť významu osobných údajov a citlivých informačných aktív v mimopracovnej oblasti a osvojiť si základné pravidlá bezpečnej manipulácie a používania IKT.

Odborný zamestnanec:

- porozumieť vybraným základným pojmom kybernetickej bezpečnosti,
- porozumieť svojej úlohe a zodpovednosti v systéme kybernetickej bezpečnosti,
- chápať význam informačných aktív s ktorými zamestnanec pracuje,
- porozumieť potrebe ochrany informácií a informačných aktív,
- osvojiť si základné pravidlá bezpečnej práce s IKT,
- rozpoznať incident a vedieť naň správne reagovať,
- porozumieť bezpečnostným politikám a používaniu bezpečnostných mechanizmov v pracovných procesoch.

Manažér:

- porozumieť vybraným základným pojmom kybernetickej bezpečnosti,
- porozumieť rizikám kybernetickej bezpečnosti v riadených procesoch,
- nadobudnúť schopnosť analyzovať požadovanú úroveň ochrany informačných aktív,
- nadobudnúť schopnosť integrovať požiadavky kybernetickej bezpečnosti do procesov a úloh podriadených zamestnancov,
- naučiť sa definovať a dohliadať na plnenie požiadaviek kybernetickej bezpečnosti pri obstaraní produktov a služieb a pri procesoch podporovaných tretími stranami.

Obsah metodiky (moduly)

Číslo modulu	Názov modulu	Časová dotácia (45 min.)	Forma stretnutia
Modul č. 1	**Úvod do kybernetickej a informačnej bezpečnosti (KIB)**	**6**	**Online / Prezenčne**
Modul č. 2	**Kritické myslenie a dezinformácie**	**8**	**Online / Prezenčne**
Modul č. 3	**Sociálne inžinierstvo**	**8**	**Online / Prezenčne**
Modul č. 4	**Bezpečnosť prevádzky a riešenie kybernetických incidentov**	**8**	**Online / Prezenčne**
Modul č. 5	**Digitálna identita a súkromie v online prostredí**	**8**	**Online / Prezenčne**
Modul č. 6	**Základy práva informačných a komunikačných technológií pre KIB I.**	**8**	**Online / Prezenčne**

Modul č. 7	**Základy práva informačných a komunikačných technológií pre KIB II.**	**8**	**Online / Prezenčne**

Poznámky

Modul č.1 - Úvod do kybernetickej a informačnej bezpečnosti (KIB)

Obsah vzdelávacieho modulu

Obsahom modulu budú základné pojmy a vzťahy v oblasti kybernetickej a informačnej bezpečnosti (KIB). Vysvetlí sa význam KIB nielen z pohľadu špecialistu v KIB ale aj používateľa IKT a online platforiem. Prejdú sa základné princípy a ukážu sa aktuálne bezpečnostné hrozby podľa ENISA Threat Landscape materiálov. V rámci praktického cvičenia sa účastníci budú venovať identifikácii aktív, hrozieb, zraniteľností a rizík. . Doplňujúco sa účastníci oboznámia so súčasným legislatívnym rámcom (zákona o kybernetickej bezpečnosti, zákona o informačných technológiách verejnej správy), mýtmi o kybernetickej bezpečnosti, ako aj pravidlami čistého stola. . .

1) Úvodné poznámky o KIB
    a) Svet okolo nás
    b) Pojem informačnej a kybernetickej bezpečnosti
2) Model KIB
    a) Aktívum
    b) Bezpečnostné hrozby
    c) Bezpečnostné zraniteľnosti
    d) Útok
    e) Útočník
    f) Riziko
    g) Bezpečnostné opatrenie
3) Bezpečnostné hrozby
    a) Aktuálne bezpečnostné hrozby
    b) Malvér
    c) Zneužitie webových sídel
    d) Sociálne inžinierstvo
    e) Botnet a DDoS
    f) Sieťové útoky
    g) Únik údajov
    h) Ransomvér
    i) Dodávateľské vzťahy
    j) Bezpečnosť umelej inteligencie (AI)
4) Právna úprava KIB
    a) Európsky právny rámec

b) Slovenský právny rámec
c) Mýty o kybernetickej bezpečnosti

5) Pravidlá čistého stola
6) Záverečná časť
    a) Diskusia
    b) Záverečné hodnotenie
    c) Spätná väzba

Odporúčané metódy

- *interaktívna prednáška s diskusiou – na vysvetlenie základných rámcov, legislatívy a technických štandardov,*
- *cvičenie – analýza rizík v organizácii,*
- *prípadové štúdie (case studies) – na analýzu reálnych bezpečnostných hrozieb a kybernetických bezpečnostných incidentov,*
- *rozhovor, diskusné metódy, riadená diskusia,*
- *gamifikovaný kvíz alebo simulácia – na overenie pochopenia hrozieb a zraniteľností.*

Metodický postup

Téma	**Podtéma**	**Materiál a pomôcky**	**Metodické poznámky**	**Hod.**
Úvodné poznámky o KIB	*Svet okolo nás* *Pojem informačnej a kybernetickej bezpečnosti*	*Prezentácia*	*Prednáška* *Prednáška*	*30 min.*
Model KIB	*Aktívum* *Bezpečnostné hrozby* *Bezpečnostné zraniteľnosti* *Útok* *Útočník* *Riziko* *Bezpečnostné opatrenie*	*Prezentácia*	*Prednáška s diskusiou* *Úloha – identifikácia základných pojmov v rozprávke*	*60 min.*

Téma	Podtéma	Materiál a pomôcky	Metodické poznámky	Hod.
Bezpečnostné hrozby	*Aktuálne bezpečnostné hrozby* *Malvér* *Zneužitie webových sídel* *Sociálne inžinierstvo* *Botnet a DDoS* *Sieťové útoky* *Únik údajov* *Ransomvér* *Dodávateľské vzťahy* *Bezpečnosť umelej inteligencie (AI)*	*Prezentácia*	*Prednáška s diskusiou*	*60 min.*
Právna úprava KIB	*Európsky právny rámec* *Slovenský právny rámec* *Mýty kybernetickej bezpečnosti*	*Prezentácia* *Portál slov-lex a eur-lex*	*Prednáška s diskusiou*	*45 min.*
Pravidlá čistého stola		*Prezentácia*	*Prednáška s diskusiou* *Úloha – analýza čistého stola a miestnosti*	*45 min.*
Záverečná časť	*Diskusia* *Záverečné hodnotenie* *Spätná väzba*	*Online test* *Spätná väzba od účastníkov.*	*Diskusia*	*30 min.*

Podklady

- *študijný materiál – prezentácia KCKB_A2_V2.1.2_Laik_M1_01_Úvod_KIB.pptx,*
- *študijný materiál – vzorová analýza rizík,*
- *študijný materiál – vzorová dopadová štúdia,*
- *študijný materiál – CTI správa o skupine útočníkov,*

- *študijný materiál – vzorová zmluva s dodávateľom,*
- *spätná väzba od účastníkov.*

Poznámky

Modul č.2 - Kritické myslenie a dezinformácie

Obsah vzdelávacieho modulu

Vzdelávací blok sa zameriava na rozvoj kritického myslenia, identifikáciu kognitívnych skreslení a odhaľovanie argumentačných faulov, ktoré často zohrávajú kľúčovú rolu v šírení dezinformácií, propagandy a konšpiračných teórií. Účastníci sa naučia analyzovať mediálne obsahy a diskusie, rozpoznať manipulatívne techniky, ako aj hodnotiť dôveryhodnosť zdrojov. Program zahŕňa teoretické prednášky doplnené interaktívnymi aktivitami ako diskusné a rolové hry, storytelling či modelové situácie. Špeciálna pozornosť sa venuje výzvam nových médií (clickbait, trolling, deepfakes, fake news) a efektívnym stratégiám ich zvládania. Cieľom je posilniť mediálnu gramotnosť účastníkov a podporiť ich schopnosť orientovať sa v online prostredí s kritickým odstupom. Výučba je postavená na aktívnom zapojení účastníkov a reflexii praktických príkladov z informačného prostredia.

1) Kritické myslenie a moderné výzvy
    a) Dezinformácie, propaganda a konšpiračné teórie.
    b) Kritické myslenie, kognitívne skreslenia a argumentačné fauly
2) Mediálna gramotnosť a zdravý pohyb v online priestore
    a. Fungovanie médií, nové (sociálne) médiá a primárne výzvy (clickbait, trolling, deepfakes, fake news).
    a) Rozpoznávanie dezinformácií a manipulácií, overovanie faktov, hodnotenie dôveryhodnosti zdrojov.

Odporúčané metódy

- *prednáška s diskusiou,*
- *storytelling,*
- *gamifikácia,*
- *audiovizuálne pomôcky,*
- *role-playing,*
- *zapojenie účastníkov.*

Metodický postup

Téma	Podtéma	Materiál a pomôcky	Metodické poznámky	Hod.
Kritické myslenie a moderné výzvy	*Kritické myslenie, kognitívne skreslenia a argumentačné fauly* *Dezinformácie, propaganda a konšpiračné teórie*	*Prezentácia*	*Prednáška s diskusiou* *Interaktívna hra „Štyri rohy“ (účastníci dostanú stanoviská a musia sa rozhodnúť o svojom postoji, pričom argumentujú svoje rozhodnutia)* *Modelová situácia „Online aktivista vs. troll“ (účastníci reagujú na komentáre a hodnotia, aké stratégie fungujú pri odpovedaní na dezinformácie)*	*90 min.* *45 min.* *45 min.*
Mediálna gramotnosť a zdravý pohyb v online priestore	*Fungovanie médií, nové (sociálne) médiá a primárne výzvy (clickbait, trolling, deepfakes, fake news)* *Rozpoznávanie dezinformácií a manipulácií, overovanie faktov, hodnotenie dôveryhodnosti zdrojov*	*Prezentácia*	*Prednáška s diskusiou* *Diskusná hra „Nájdi chybu“ (účastníci analyzujú vopred pripravené argumenty s logickými chybami a diskutujú, v čom sú problematické)* *Interaktívna prednáška s príkladmi z médií (analyzovanie reálnych správ a diskusií s cieľom identifikovať argumentačné chyby a manipulatívne techniky)*	*90 min.* *30 min.* *30 min.*
Záverečná časť	*Diskusia* *Záverečné hodnotenie* *Spätná väzba*	*Online test* *Spätná väzba od účastníkov.*	*Diskusia*	*30 min.*

Podklady

- *študijný materiál – prezentácia KCKB_A2_V2.1.2_Laik_M2_01_Kriticke_myslenie.pptx,*
- *spätná väzba od účastníkov.*

Poznámky

Modul č. 3 – Sociálne inžinierstvo

Obsah vzdelávacieho modulu

Vzdelávací modul sa zameriava na problematiku sociálneho inžinierstva ako jednej z najčastejších foriem kybernetických útokov zameraných na manipuláciu používateľov. V úvode poukazujeme na rozdiel medzi realitou a jej vnímaním, pričom si predstavíme aj rôzne princípy vplyvu a typy myslenia. Účastníci sa oboznámia so základnými princípmi a formami útokov (phishing, spear phishing, vishing, smishing, baiting, spam, scam, quishing, online podvody) a naučia sa rozpoznávať znaky podvodných emailov. Osobitná pozornosť je venovaná analýze obsahu správ, pričom modul zahŕňa aj viaceré praktické ukážky reálnych phishingových emailov.. Súčasťou výučby je interaktívny phishingový test a diskusia o najnovších trendoch v oblasti podvodnej komunikácie. Cieľom je zvýšiť odolnosť účastníkov voči manipulatívnym technikám a posilniť ich schopnosť efektívne reagovať na podozrivé správy.

1) Úvod do sociálneho inžinierstva
    a) Základné princípy.
    b) Realita vs. vnímanie reality
    c) Princípy vplyvu
    d) Typy myslenia
2) Formy sociálneho inžinierstva
    a) Phishing / Spear Phishing,
    b) Vishing,
    c) Smishing,
    d) Baiting,
    e) Spam,
    f) Scam,
    g) Quishing,
    h) Online podvody
3) Znaky podvodného emailu
    a) Prílohy,
    b) Odkazy,
    c) Sémantická stránka textu,
    d) Emailová adresa odosielateľa,
    e) Urgencia,
    f) Oslovenie,
    g) Podpis.
4) Príklady sociálneho inžinierstva
    a) Aktuálne trendy,

b) Pravidlá ochrany pred podvodnými správami.
c) Analýza reálnych prípadov a diskusia

5) Záverečná časť
   d) Diskusia
   e) Záverečné hodnotenie
   f) Spätná väzba

Odporúčané metódy

- *prednáška s diskusiou,*
- *cvičenie,*
- *rozhovor, diskusné metódy, riadená diskusia,*
- *samostatná práca.*

Metodický postup

Téma	**Podtéma**	**Materiál a pomôcky**	**Metodické poznámky**	**Hod.**
Úvod do sociálneho inžinierstva	*Základné princípy* *Realita vs. vnímanie reality* *Princípy vplyvu* *Typy myslenia*	*Prezentácia*	*Prednáška*	*60 min*
Formy sociálneho inžinierstva	*Phishing/ Spear Phihing* *Vishing* *Smishing* *Baiting* *Spam* *Scam* *Quishing* *Online podvody*	*Prezentácia*	*Prednáška s diskusiou*	*90 min*

Téma	Podtéma	Materiál a pomôcky	Metodické poznámky	Hod.
Znaky podvodného emailu	*Prílohy* *Odkazy* *Sémantická stránka textu* *Emailová adresa odosielateľa* *Urgencia* *Oslovenie* *Podpis*	*Prezentácia* *Prezentácia*	*Prednáška s diskusiou*	*30 min*
Príklady sociálneho inžinierstva	*Aktuálne trendy* *Pravidlá ochrany pred podvodnými správami.* *Analýza reálnych prípadov a diskusia*	*Prezentácia* *Phishingový test - https://csirt.upjs.sk/phishing/* *Prípadové štúdie*	*Prednáška s diskusiou* *Workshop (phishingový test)*	*45 min* *45 min* *60 min*
Záverečná časť	*Diskusia* *Záverečné hodnotenie* *Spätná väzba*	*Online test* *Spätná väzba od účastníkov.*	*Diskusia*	*30 min.*

Podklady

- *študijný materiál – prezentácia KCKB_A2_V2.1.2_Laik_M3_01_Socialne_inžinierstvo.pptx,*
- *spätná väzba od účastníkov.*

Poznámky

Modul č. 4 - Bezpečnosť prevádzky a riešenie kybernetických incidentov

Obsah vzdelávacieho modulu

Obsah modulu sa zameriava na základné aspekty bezpečnej práce s IKT vrátane práce s citlivými údajmi. Ukážeme si, ako sa prejavuje škodlivý kód (malvér), najmä však ransomvér. Účastníci získajú prehľad o typoch malvéru, ich šírení a vplyve na zariadenia a infraštruktúru. Modul sa zameriava aj na bezpečnosť mobilných zariadení (najmä s operačným systémom Android a IOS) a v rámci neho si účastníci budú môcť prejsť základné bezpečnostné nastavenia týchto zariadení. V rámci modulu sa zameriame aj na spôsob riešenia bezpečnostných incidentov z pohľadu používateľa. V rámci modulu budú vysvetlené aj niektoré štandardne používané bezpečnostné opatrenia, ako je napr. vzdialený prístup k zariadeniu, resp. používania antimalvérových riešení.

1) Úvod do riešenia bezpečnostných incidentov
    a) Motivácia.
    b) Základné pojmy.
    c) Bezpečnostný incident (Udalosť/ Bezpečnostná udalosť/ Bezpečnostný incident).
    d) Právny rámec.
    e) Kontinuita činnosti.
2) Riešenie bezpečnostných incidentov
    a) Fázy riešenia BI.
    b) Taxonómia.
    c) Komunikácia BI.
    d) Prípadová štúdia.
    e) Role-play.
3) Malvér
    a) Úvod.
    b) Typy malvéru.
    c) Spôsoby šírenia.
    d) Detekcia malvéru.
    e) Ransomvér.
4) Kryptológia
    a) Motivácia
    b) História a súčasnosť
    c) Symetrická kryptografia
    d) Asymetrická kryptografia

e) Kryptoanalýza
f) Hešovacie funkcie
g) Podpisovanie
h) Certifikáty a certifikačné autority, životný cyklus
i) Podpis, elektronický podpis, zdokonalený a kvalifikovaný elektronický podpis

5) Bezpečnosť mobilných zariadení
    a) Motivácia.
    b) Priebeh útokov na mobilné zariadenia.
    c) Povolenia.
    d) Bezpečný telefón.
    e) Workshop zabezpečenia telefónu.
6) Záverečná časť
    a) Diskusia
    b) Záverečné hodnotenie
    c) Spätná väzba

Odporúčané metódy

- *prednáška s diskusiou,*
- *cvičenie – práca s mobilnými zariadeniami,*
- *gamifikácia,*
- *tabletop cvičenia a role-play scenáre – pre trénovanie reakcií na kybernetické bezpečnostné incidenty.*

Metodický postup

Téma	**Podtéma**	**Materiál a pomôcky**	**Metodické poznámky**	**Hod.**
Úvod do riešenia bezpečnostných incidentov	*Motivácia* *Základné pojmy* *Bezpečnostný incident (Udalosť/ Bezpečnostná udalosť/ Bezpečnostný incident)* *Právny rámec* *Kontinuita činnosti*	*Prezentácia*	*prednáška*	*60 min*

Téma	Podtéma	Materiál a pomôcky	Metodické poznámky	Hod.
Riešenie bezpečnostných incidentov	*Fázy riešenia BI* *Taxonómia* *Komunikácia BI* *Prípadová štúdia* *Role-play*	*Prezentácia*	*Prednáška* *Tabletop cvičenie* *Role-play*	*90 min*
Malvér	*Úvod* *Typy malvéru* *Spôsoby šírenia* *Detekcia malvéru* *Ransomvér*	*Prezentácia*	*Prednáška* *Workshop* *Ukážky malvéru* *Ukážky ransomvéru*	*60 min*
Kryptológia	*Motivácia* *História a súčasnosť* *Symetrická kryptografia* *Asymetrická kryptografia* *Kryptoanalýza* *Hešovacie funkcie* *Podpisovanie* *Certifikáty a certifikačné autority, životný cyklus* *Podpis, elektronický podpis, zdokonalený a kvalifikovaný elektronický podpis*	*Prezentácia* *Nástroj Cyberchef (https://gchq.github.io/CyberChef/)*	*Prednáška* *Workshop*	*60 min*

Téma	Podtéma	Materiál a pomôcky	Metodické poznámky	Hod.
Bezpečnosť mobilných zariadení	*Motivácia* *Priebeh útokov na mobilné zariadenia* *Povolenia* *Bezpečný telefón* *Workshop zabezpečenia telefónu*	*Prezentácia*	*Prednáška* *Workshop*	*60 min*
Záverečná časť	*Diskusia* *Záverečné hodnotenie* *Spätná väzba*	*Online test* *Spätná väzba od účastníkov.*	*Diskusia*	*30 min.*

Podklady

- *študijné materiály - Prezentácia KCKB_A2_V2.1.2_Laik_M4_01_Reaktívne_ proaktívne_činnosti.pptx,*
- *Hra Backdoor and Breaches,*
- *spätná väzba od účastníkov.*

Poznámky

Modul č. 5 – Digitálna identita a súkromie v online prostredí

Obsah vzdelávacieho modulu

Modul sa zameria na to, čo znamená digitálna identita a akým spôsobom vplýva na bezpečnosť používateľov. Predstavíme predpoklady a hlavné oblasti digitálnej transformácie spoločnosti s dôrazom na človeka a úlohu štátu, pričom účastníci získajú prehľad o nástrojoch na ochranu digitálnej identity, ako sú eSignature, eTimestamp a eID. Budeme sa venovať rôznym spôsobom preukázania identifikácie, najmä použitiu hesiel vrátane vysvetlenia viacfaktorového overenia. V rámci tohto modulu si účastníci taktiež vyskúšajú prácu s manažérmi hesiel. Súčasťou školenia bude vysvetlenie bezpečnostných rizík v online prostredí a aplikácie bezpečnostných opatrení. Okrem toho získajú prehľad o základných princípoch ochrany digitálneho súkromia, vrátane rôznych foriem súkromia, používania cookies a zabezpečenia online platieb.

1) Digitálna transformácia spoločnosti a verejného priestoru
    a) Predpoklady a oblasti digitálnej transformácie spoločnosti.
    b) Človek v centre pozornosti digitálnej transformácie spoločnosti.
    c) Government ako súčasť digitálnej transformácie.
2) Digitálna identita
    a) Digitálna identita – vymedzenie a význam.
    b) Nástroje ochrany digitálnej identity (eSignature, eTimestamp, eID, ...).
3) Digitálne súkromie
    a) Digitálne súkromie – vymedzenie a význam.
    b) Ochrana digitálneho súkromia (individuálne, informačné a komunikačné súkromie; základné princípy ochrany digitálneho súkromia).
    c) Bezpečnostné opatrenia
4) Bezpečnosť hesiel
    a) Tvorba Hesiel
    b) Manažér hesiel
    c) Viacfaktorová autentifikácia
5) Prípadové štúdie
    a) Aktuálne trendy
    b) Analýza prípadových štúdií
6) Záverečná časť
    a) Diskusia
    b) Záverečné hodnotenie
    c) Spätná väzba

Odporúčané metódy

- *prednáška s diskusiou,*
- *rozhovor, diskusné metódy, riadená diskusia,*
- *samostatná práca.*

Metodický postup

Téma	**Podtéma**	**Materiál a pomôcky**	**Metodické poznámky**	**Hod.**
Digitálna transformácia spoločnosti a verejného priestoru	*Predpoklady a oblasti digitálnej transformácie spoločnosti* *Človek v centre pozornosti digitálnej transformácie spoločnosti* *Government ako súčasť digitálnej transformácie*	*Prezentácia*		*60 min*
Digitálna identita	Digitálna identita – vymedzenie a význam Nástroje ochrany digitálnej identity – eSignature, eTimestamp, eID, ...	*Prezentácia*		*60 min.*

Téma	Podtéma	Materiál a pomôcky	Metodické poznámky	Hod.
Digitálne súkromie	*Digitálne súkromie – vymedzenie a význam* *Ochrana digitálneho súkromia (individuálne, informačné a komunikačné súkromie; základné princípy ochrany digitálneho súkromia)* *Bezpečnostné opatrenia*	*Prezentácia*		*60 min.*
Bezpečnosť hesiel	*Tvorba Hesiel* *Manažér hesiel* *Viacfaktorová autentifikácia*	*Tester hesiel - https://csirt.upjs.sk/hesla/*	*prednáška* *cvičenie*	*30 min.*
Prípadové štúdie	*Aktuálne trendy* *Analýza prípadových štúdií*	*Prezentácia*	*Prednáška* *Diskusia*	*30 min.*
Záverečná časť	*Diskusia* *Záverečné hodnotenie* *Spätná väzba*	*Online test* *Spätná väzba od účastníkov.*	*Diskusia*	*30 min.*

Podklady

- *študijné materiály - Prezentácia KCKB_A2_V2.1.2_Laik_M5_01_Digitalna_identita.pptx,*
- *spätná väzba od účastníkov.*

Poznámky

Modul č. 6 - Základy práva informačných a komunikačných technológií pre KIB I.

Obsah vzdelávacieho modulu

Vzdelávací modul sa zameriava na kľúčové právne aspekty informačných a komunikačných technológií (IKT) a ich uplatnenie v praxi. Úvodná časť poskytuje vysvetlenie pojmu práva IKT a základných princípov, ktoré túto oblasť formujú. Nasleduje tematický blok venovaný elektronickým právnym úkonom a službám vytvárajúcim dôveru, vrátane elektronického podpisu, elektronickej pečate, digitálneho podpisu, certifikátov a elektronického doručovania, ako aj prehľadu poskytovateľov dôveryhodných služieb. Ďalšia časť sa zameriava na ochranu súkromia a osobných údajov – od definície osobného údaju, cez procesy jeho spracovania, cezhraničného prenosu a zabezpečenia, až po práva dotknutých osôb a príklady z praxe. Štvrtý tematický okruh je venovaný elektronickému obchodu, jeho pojmu a charakteristike, typom a špecifikám, výhodám a nevýhodám elektronického obchodovania, ako aj právnym otázkam elektronických zmlúv. Súčasťou modulu sú aj prípadové štúdie, ktoré umožňujú aplikovať teoretické poznatky na reálne situácie, a záverečná časť zameraná na diskusiu, zhodnotenie získaných vedomostí a spätnú väzbu od účastníkov.

1) Právo informačných a komunikačných technológií
   a) Pojem práva IKT.
   b) Základné princípy.
2) Duševné vlastníctvo a jeho ochrana
   a) Pojem a druhy duševného vlastníctva – autorské práva, priemyselné práva, práva k databázam, softvéru a multimédiám.
   b) Právna ochrana duševného vlastníctva v prostredí IKT.
   c) Porušenie práv duševného vlastníctva a jeho dôsledky.
3) Ochrana súkromia a osobných údajov
   a) Definícia osobného údaju.
   b) Spracovanie osobných údajov.
   c) Subjekty v oblasti ochrany osobných údajov – prevádzkovateľ, sprostredkovateľ, dotknutá osoba.
   d) Práva dotknutých osôb.
   e) Bezpečnosť osobných údajov.
   f) Príklady z praxe.
4) Elektronické právne úkony a služby vytvárajúce dôveru
   a) Elektronické právne úkony a elektronický dokument.
   b) Služby vytvárajúce dôveru – elektronický podpis, elektronická pečať, digitálny podpis, certifikát, elektronické doručovanie.
   c) Poskytovatelia dôveryhodných služieb.

5) Prípadové štúdie
    a) Analýza prípadových štúdií
6) Záverečná časť
    a) Diskusia
    b) Záverečné hodnotenie
    c) Spätná väzba

Odporúčané metódy

- *prednáška s diskusiou,*
- *samostatná práca.*

Metodický postup

Téma	**Podtéma**	**Materiál a pomôcky**	**Metodické poznámky**	**Hod.**
Právo informačných a komunikačných technológií	*Pojem práva IKT* *Základné princípy*	*Prezentácia*	*Prednáška s diskusiou*	*30 min.*
Elektronické právne úkony a služby vytvárajúce dôveru	*Elektronické právne úkony, elektronický dokument.* *Služby vytvárajúce dôveru. Elektronický podpis, elektronická pečať, digitálny podpis, certifikát, elektronické doručovanie.* *Poskytovatelia dôveryhodných služieb.*	*Prezentácia*	*Prednáška s diskusiou*	*90 minút*

Téma	Podtéma	Materiál a pomôcky	Metodické poznámky	Hod.
Ochrana súkromia a osobných údajov	*Definícia osobného údaju.* *Spracovanie osobných údajov,* *Subjekty v oblasti ochrany osobných údajov* *Práva dotknutých osôb.* *Bezpečnosť osobných údajov.* *Príklady z praxe.*	*Prezentácia*	*Prednáška s diskusiou*	*90 minút*
Elektronický obchod	*Pojem a charakteristika elektronického obchodu.* *Typy elektronického obchodu. Výhody a nevýhody elektronického obchodovania.* *Zmluvy uzatvorené prostredníctvom elektronických prostriedkov.* *Typy elektronických zmlúv.*	*Prezentácia*	*Prednáška a workshop*	*90 minút*
Prípadové štúdie	*Analýza prípadových štúdií*	*Prezentácia*	*Prednáška a diskusia*	*30 min.*
Záverečná časť	*Diskusia* *Záverečné hodnotenie* *Spätná väzba*	*Online test* *Spätná väzba od účastníkov.*	*Diskusia*	*30 min.*

Podklady

- *študijné materiály - Prezentácia KCKB_A2_V2.1.2_Laik_M6_01_Právo_IKT_I.pptx,*
- *spätná väzba od účastníkov.*

Poznámky

Modul č. 7 - Základy práva informačných a komunikačných technológií pre KIB II.

Obsah vzdelávacieho modulu

Modul sa zameriava na problematiku duševného vlastníctva a trestnoprávnych aspektov kybernetickej kriminality. Účastníci sa oboznámia s pojmom a druhmi duševného vlastníctva vrátane autorských práv, priemyselných práv a práv k databázam, softvéru a multimédiám, ako aj s právnou ochranou v prostredí IKT a dôsledkami porušovania týchto práv. V trestnoprávnej časti sa preberajú hmotnoprávne aj procesné aspekty kybernetickej kriminality, vrátane špecifík jej vyšetrovania a dokazovania v digitálnom prostredí. Súčasťou modulu sú prípadové štúdie, ktoré umožňujú prepojenie teoretických vedomostí s praxou, a záverečná diskusia so zhodnotením získaných poznatkov a spätnou väzbou od účastníkov.

1) Trestnoprávne aspekty kybernetickej kriminality
    a) Trestnoprávne (hmotnoprávne) aspekty kybernetickej kriminality.
    b) Trestnoprocesné aspekty kybernetickej kriminality.
2) Elektronický obchod
    c) Pojem a charakteristika elektronického obchodu.
    d) Typy elektronického obchodu.
    e) Výhody a nevýhody elektronického obchodovania.
    f) Zmluvy uzatvorené prostredníctvom elektronických prostriedkov.
    g) Typy elektronických zmlúv.
3) Prípadové štúdie
    a) Analýza prípadových štúdií
4) Záverečná časť
    a) Diskusia
    b) Záverečné hodnotenie
    c) Spätná väzba

Odporúčané metódy

- *prednáška s diskusiou,*
- *cvičenie.*

Metodický postup

Téma	Podtéma	Materiál a pomôcky	Metodické poznámky	Hod.
Duševné vlastníctvo a jeho ochrana	*Pojem a druhy duševného vlastníctva – autorské práva, priemyselné práva, práva k databázam, softvéru a multimédiám.* *Právna ochrana duševného vlastníctva v prostredí IKT* *Porušenie práv duševného vlastníctva a jeho dôsledky.*	*Prezentácia*	*Prednáška s diskusiou*	*90 min*
Trestnoprávne aspekty kybernetickej kriminality	*Trestnoprávne (hmotnoprávne) aspekty kybernetickej kriminality* *Trestnoprocesné aspekty kybernetickej kriminality*	*Prezentácia*	*Prednáška s diskusiou* *Prednáška s diskusiou*	*180 minút*
Prípadové štúdie	*Analýza prípadových štúdií*	*Prezentácia*	*Prednáška a diskusia*	*60 min.*
Záverečná časť	*Diskusia* *Záverečné hodnotenie* *Spätná väzba*	*Online test* *Spätná väzba od účastníkov.*	*Diskusia*	*30 min.*

Prílohy

- *študijné materiály - Prezentácia KCKB_A2_V2.1.2_Laik_M7_01_Právo_IKT_II.pptx,*
- *spätná väzba od účastníkov.*

Poznámky