;

Metodika pre lektora

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

verzia 1.0

Košice, marec 2025

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**	**6**	**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 v ich organizáciách. Doplňujúco sa účastníci oboznámia so súčasným legislatívnym rámcom (zákona o kybernetickej bezpečnosti, zákona o informačných technológiách verejnej správy), princípmi systému riadenia KIB podľa noriem ISO, základmi riadenia kontinuity činností, ako aj taktikami a technikami útočníkov vrátane rámcov MITRE ATT&CK a Cyber Kill Chain.

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) Právna úprava KIB
    a) Európsky právny rámec
    b) Slovenský právny rámec
    c) Smernica NIS 2
    d) Zákon o KB
    e) Zákon o ITVS
4) Taktiky a techniky útočníkov
    a) Analýza skupín útočníkov
    b) Cyber kill chain
    c) MITRE ATT&CK rámec
5) Systém riadenia KIB
    a) Úvod a ISO normy

b) Zavedenie systému riadenia
c) Implementácia a prevádzka

6) Riadenie kontinuity činností
   a) Kontinuita činností
   b) Dôležité pojmy
   c) Riadenie kontinuity činností
7) Dodávateľské vzťahy
   a) Hrozba dodávateľských vzťahov
   b) Vzťah s tretími stranami
8) Riadenie bezpečnostných rizík
   a) Bezpečnostné riziko
   b) Proces riadenia rizík
   c) Identifikácia aktív
   d) Identifikácia hrozieb
   e) Identifikácia zraniteľností
   f) Analýza rizík
   g) Vyhodnotenie rizík

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.*

Téma	Podtéma	Materiál a pomôcky	Metodické poznámky	Hod.
Model KIB	*Aktívum* *Bezpečnostné hrozby* *Bezpečnostné zraniteľnosti* *Útok* *Útočník* *Riziko* *Bezpečnostné opatrenie*	*Prezentácia*	*Prednáška s diskusiou*	*60 min.*
Právna úprava KIB	*Európsky právny rámec* *Slovenský právny rámec* *Smernica NIS 2* *Zákon o KB* *Zákon o ITVS*	*Prezentácia* *Portál slov-lex a eur-lex*	*Prednáška s diskusiou*	*45 min.*
Taktiky a techniky útočníkov	*Analýza skupín útočníkov* *Cyber kill chain* *MITRE ATT&CK rámec*	*Prezentácia* *Mitre Attack rámec* *CTI správa o skupine útočníkov*	*Prednáška s diskusiou* *Prednáška s diskusiou* *Workshop – analýza činnosti vybranej skupiny (podľa CTI správy o skupine útočníkov)*	*45 min.*

Téma	Podtéma	Materiál a pomôcky	Metodické poznámky	Hod.
Systém riadenia KIB	*Úvod a ISO normy* *Zavedenie systému riadenia* *Implementácia a prevádzka*	*Prezentácia* *ISO 27000 normy*	*Prednáška s diskusiou* *Prednáška s diskusiou* *Prednáška s diskusiou*	*30 min.*
Riadenie kontinuity činností	*Kontinuita činností* *Dôležité pojmy* *Riadenie kontinuity činností*	*Prezentácia* *Vzorová dopadová analýza*	*Prednáška s diskusiou* *Workshop - Dopadová analýza*	*30 min.*
Dodávateľské vzťahy	*Hrozba dodávateľských vzťahov* *Vzťah s tretími stranami*	*Prezentácia* *Ukážka vzorovej zmluvy s dodávateľom*	*Prednáška s diskusiou*	*30 min.*
Riadenie bezpečnostných rizík	*Bezpečnostné riziko* *Proces riadenia rizík* *Identifikácia aktív* *Identifikácia hrozieb* *Identifikácia zraniteľností* *Analýza rizík* *Vyhodnotenie rizík*	*Prezentácia* *Ukážkový material – analýza rizík*	*Prednáška s diskusiou* *Prednáška s diskusiou* *Workshop – identifikácia aktív* *Workshop – identifikácia hrozieb* *Workshop – identifikácia zraniteľností* *Workshop – analýza rizík* *Workshop – vyhodnotenie rizík*	*90 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 aktuálneho mediálneho prostredia.

1) Kritické myslenie, kognitívne skreslenia a argumentačné fauly
    a) Dezinformácie, propaganda a konšpiračné teórie.
    b) Mediálna gramotnosť a zdravý pohyb v online priestore.
2) Dezinformácie, propaganda a konšpiračné teórie
    a) Fungovanie médií, nové (sociálne) médiá a primárne výzvy (clickbait, trolling, deepfakes, fake news).
    b) 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* *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.* *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* *Interaktívna hra „Štyri rohy“ (účastníci dostanú stanovisku 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.*

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. Účastníci sa oboznámia so základnými princípmi a formami útokov (phishing, spear phishing, vishing, smishing, baiting, spam) a naučia sa rozpoznávať znaky podvodných emailov. Osobitná pozornosť je venovaná analýze obsahu správ, ako aj technickej analýze emailových hlavičiek vrátane protokolov SPF, DKIM a DMARC. Modul zahŕňa praktické ukážky, analýzy reálnych phishingových emailov a prácu s nástrojmi ako MXToolbox, Verifalia či Whois. 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.
2) Formy sociálneho inžinierstva
    a) Phishing / Spear Phishing,
    b) Vishing,
    c) Smishing,
    d) Baiting,
    e) Spam.
3) Znaky podvodného emailu
    a) Prílohy,
    b) Odkazy,
    c) Sémantická stránka textu,
    d) Emailová adresa odosielateľa,
    e) Urgencia,
    f) Oslovenie,
    g) Podpis.
4) Príklady podvodných emailov
    a) Aktuálne trendy,
    b) Pravidlá ochrany pred podvodnými správami.
5) Analýza emailovej hlavičky
    a) SPF,
    b) DKIM,
    c) DMARC,
    d) Emailová adresa odosielateľa,

e) IP adresa,
f) Nástroje na analýzu (MXToolbox, Verifalia, Whois).

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*	*Prezentácia*	*Prednáška*	*15 min*
Formy sociálneho inžinierstva	*Phishing/ Spear Phihing* *Vishing* *Smishing* *Baiting* *Spam*	*Prezentácia*	*Prednáška s diskusiou*	*30 min*
Znaky podvodného emailu	*Prílohy* *Odkazy* *Sémantická stránka textu* *Emailová adresa odosielateľa* *Urgencia* *Oslovenie* *Podpis*	*Prezentácia* *Prezentácia*	*Prednáška s diskusiou*	*30 min*

Téma	Podtéma	Materiál a pomôcky	Metodické poznámky	Hod.
Príklady podvodných emailov	*Aktuálne trendy* *Pravidlá ochrany pred podvodnými správami.*	*Prezentácia* *Phishingový test - https://csirt.upjs.sk/phishing/*	*Prednáška s diskusiou* *Workshop (phishingový test)*	*30 min + 15 min*
Analýza emailovej hlavičky	*SPF* *DKIM* *DMARC* *Emailová adresa odosielateľa* *IP adresa* *Nástroje na analýzu (MXToolbox, Verifalia, Whois)*	*Prezentacia*	*Workshop* *prednáška*	*90 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) Ciele informačnej bezpečnosti.
    e) Právny rámec.
    f) 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) Analýza malvéru.
    e) Ransomvér.
4) Bezpečnosť mobilných zariadení
    a) Motivácia.
    b) Priebeh útokov na mobilné zariadenia.
    c) Povolenia.

d) Bezpečný telefón.
e) Workshop zabezpečenia telefónu.

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)* *Ciele informačnej bezpečnosti* *Právny rámec* *Kontinuita činnosti*	*Prezentácia*	*prednáška*	*60 min*
Riešenie bezpečnostných incidentov	*Fázy riešenia BI* *Taxonómia* *Komunikácia BI* *Prípadová štúdia* *Role-play*	*Prezentácia* *Hra Backdoor and Breaches*	*Prednáška* *Tabletop cvičenie* *Role-play*	*90 min*

Téma	Podtéma	Materiál a pomôcky	Metodické poznámky	Hod.
Malvér	*Úvod* *Typy malvéru* *Spôsoby šírenia* *Analýza malvéru* *Ransomvér*	*Prezentácia*	*Prednáška* *Workshop*	*60 min*
Bezpečnosť mobilných zariadení	*Motivácia* *Priebeh útokov na mobilné zariadenia* *Povolenia* *Bezpečný telefón* *Workshop zabezpečenia telefónu*	*Prezentácia*	*Prednáška* *Workshop*	*60 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).

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*		*120 min.*
Digitálne súkromie	*Digitálne súkromie – vymedzenie a význam* *Ochrana digitálneho súkromia (individuálne, informačné a komunikačné súkromie; základné princípy ochrany digitálneho súkromia)*	*Prezentácia*		*60 min.*

Téma	Podtéma	Materiál a pomôcky	Metodické poznámky	Hod.
Bezpečnosť hesiel	*Tvorba Hesiel* *Manažér hesiel* *Viacfaktorová autentifikácia*	*Tester hesiel - https://csirt.upjs.sk/hesla/*	*prednáška* *cvičenie*	*30 min.* *30 min.*
Digitálne súkromie	*Bezpečnostné opatrenia* *Bezpečnosť online platieb* *Osobný údaj* *Cookies*	*Prezentácia*	*workshop* *konzultácie*	*30 min.* *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 právne aspekty informačných a komunikačných technológií (IKT), pričom ponúka úvod do základných pojmov a oblastí práva IKT. Osobitná pozornosť je venovaná dôveryhodným službám, ako sú elektronický podpis, certifikáty a digitálne právne úkony, ktoré zohrávajú kľúčovú úlohu v elektronickej komunikácii. Modul tiež objasňuje problematiku duševného vlastníctva a jeho právnej ochrany v digitálnom prostredí. Druhá časť sa venuje ochrane súkromia a osobných údajov, vrátane práv dotknutých osôb, cezhraničného prenosu údajov a bezpečnostných opatrení. Tretia tematická oblasť pokrýva elektronický obchod, jeho typy, špecifiká elektronických zmlúv a právne výzvy, ktoré z neho vyplývajú. Cieľom je poskytnúť účastníkom praktický právny rámec pre orientáciu v digitálnom svete.

1) Právo informačných a komunikačných technológií (úvod, pojem, vymedzenie IKT)
    a) Dôveryhodné služby a elektronický podpis – služby vytvárajúce dôveru, poskytovatelia dôveryhodných služieb, elektronické právne úkony, elektronický dokument a elektronický podpis, elektronická pečať, digitálny podpis, certifikát.
    b) Duševné vlastníctvo a jeho ochrana.
2) Ochrana súkromia a osobných údajov
    a) Definícia osobného údaju. Subjekty v oblasti ochrany osobných údajov - prevádzkovateľ, sprostredkovateľ, dotknutá osoba. Práva dotknutých osôb.
    b) Spracovanie osobných údajov, cezhraničný prenos údajov, bezpečnosť osobných údajov, kódexy správania, certifikácia. Uchovávanie údajov (data retention).
3) Elektronický obchod
    a) Pojem a charakteristika elektronického obchodu.
    b) Typy elektronického obchodu.
    c) Výhody a nevýhody elektronického obchodovania.
    d) Zmluvy uzatvorené prostredníctvom elektronických prostriedkov.
    e) Typy elektronických zmlúv.

Odporúčané metódy

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

Metodický postup

Téma	Podtéma	Materiál a pomôcky	Metodické poznámky	Hod.
Právo informačných a komunikačných technológií (úvod, pojem, vymedzenie IKT).	*Dôveryhodné služby a elektronický podpis – služby vytvárajúce dôveru, poskytovatelia dôveryhodných služieb, elektronické právne úkony, elektronický dokument a elektronický podpis, elektronická pečať, digitálny podpis, certifikát* *Duševné vlastníctvo a jeho ochrana*	*Prezentácia*	*Prednáška s diskusiou* *Prednáška s diskusiou*	*90 minút* *90 minút*
Ochrana súkromia a osobných údajov	*Definícia osobného údaju. Subjekty v oblasti ochrany osobných údajov - prevádzkovateľ, sprostredkovateľ, dotknutá osoba. Práva dotknutých osôb. Spracovanie osobných údajov, cezhraničný prenos údajov, bezpečnosť osobných údajov, kódexy správania, certifikácia. Uchovávanie údajov (data retention).*	*Prezentácia*	*Prednáška s diskusiou*	*120 minút*

Téma	Podtéma	Materiál a pomôcky	Metodické poznámky	Hod.
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* *Cvičenie*	*90 minút*

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 venuje právnym a trestnoprávnym aspektom kybernetickej bezpečnosti a kybernetickej kriminality. Účastníci sa oboznámia s pojmom kybernetického bezpečnostného incidentu, úlohami CSIRT/CERT tímov, ako aj s procesmi notifikácie a zdieľania incidentov v národnom aj medzinárodnom kontexte. Dôraz sa kladie na právne mechanizmy ochrany v digitálnom priestore vrátane medzinárodnoprávnych otázok, ako je rozhodné právo či právomoc pri cezhraničných útokoch. Zároveň sa rozoberajú trestnoprávne a procesné aspekty postihovania kybernetickej kriminality, vrátane špecifík vyšetrovania a dokazovania v digitálnom prostredí.

1) Právne aspekty kybernetickej bezpečnosti
    a) Pojem kybernetického bezpečnostného incidentu.
    b) CSIRT/CERT tímy.
    c) Notifikácia a riešenie kybernetických bezpečnostných incidentov.
    d) Zdieľanie bezpečnostných incidentov.
    e) Medzinárodnoprávne aspekty kybernetickej bezpečnosti (medzinárodná právomoc, rozhodné právo).

2) Trestnoprávne aspekty kybernetickej kriminality
    a) Trestnoprávne (hmotnoprávne) aspekty kybernetickej kriminality.
    b) Trestnoprocesné aspekty kybernetickej kriminality.

Odporúčané metódy

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

Metodický postup

Téma	Podtéma	Materiál a pomôcky	Metodické poznámky	Hod.
Právne aspekty kybernetickej bezpečnosti	*Pojem kybernetického bezpečnostného incidentu. CSIRT/CERT tímy. Notifikácia a riešenie kybernetických bezpečnostných incidentov. Zdieľanie bezpečnostných incidentov.* *Medzinárodnoprávne aspekty kybernetickej bezpečnosti (medzinárodná právomoc, rozhodné právo).*	*Prezentácia*	*Prednáška s diskusiou* *Prednáška s diskusiou* *Workshop - modelový prípad*	*120 minút* *60 minút*
Trestnoprávne aspekty kybernetickej kriminality	*Trestnoprávne (hmotnoprávne) aspekty kybernetickej kriminality* *Trestnoprocesné aspekty kybernetickej kriminality*	*Prezentácia*	*Prednáška s diskusiou* *Prednáška s diskusiou*	*90 minút* *90 minút*

Prílohy

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

Poznámky