Predmet: Informačná bezpečnost

Charakteristika predmetu

Predmet podáva základné informácie o informačnej bezpečnosti. Dotýka sa základných prvkov informačnej bezpečnosti vhodne spracovaných pre žiaka strednej školy. Predmet je rozdelený do úvodu a štyroch oblastí - bezpečnosť počítačovej siete, bezpečnosti operačného systému, bezpečnosti aplikácií a bezpečnosti údajov a používateľov.

Cieľ predmetu

Cieľom predmetu je, aby žiak získal znalosti a zručnosti, na základe ktorých bude ovládať nasledovné špecializované činnosti:

- poznať koncepciu informačnej bezpečnosti a jej aplikačné možnosti
- vedieť posúdiť a identifikovať bezpečnostné aktíva, zraniteľnosti, hrozby, analyzovať a vyhodnotiť mieru bezpečnostného rizika
- posúdiť bezpečnosť počítačovej siete, poznať bezpečnostné hrozby v počítačovej sieti vzhľadom na použité médium – káblové pripojenie, WiFi pripojenie a mobilné pripojenie, zhodnotiť bezpečnostné riziko v prípade pripojenia do neznámej počítačovej siete
- vedieť posúdiť bezpečnosť pripojenia, poznať hrozby zo siete, poznať možnosti šifrovaných dát pri prenose, poznať úlohy správcu počítačovej siete a etiku pri správe siete
- poznať vhodné správanie používateľa v počítačovom systémy, zodpovednosť administrátora za počítačový systém, poznať odporúčania pre používanie hesiel
- poznať bezpečnú a efektívnu prácu s operačným systémom, poznať a posúdiť bezpečnostné hrozby a zraniteľnosti v operačnom systéme, rozpoznať jednotlivé druhy škodlivých programov a princípov proaktívnej a reaktívnej ochrany voči ním
- ovládať bezpečnosť aplikácií, ovládanie filtrovania webového obsahu u klienta a na sieti, škodlivý softvér na webe, uvedomenie si dôležitosti nezverejňovania dôverných informácií,
- odhalenie pravej a falošnej identity, poznať podstatu symetrickej a asymetrickej kryptografie, bezpečnú elektronickú poštu, bezpečnú mobilnú komunikáciu, bezpečnú a efektívnu elektronickú komunikáciu so štátom pomocou elektronickej identifikačnej karty
- poznať bezpečnosť údajov a používateľa, zálohovanie, obnovu a likvidáciu údajov, poznať taktiky sociálneho inžinierstva a kybernetickej kriminality,

ovládať zásady identifikácie sociálneho inžinierstva, poznať pojem počítačovej kriminality a jednotlivé trestné činy, identifikovať počítačové trestný činy v digitálnom priestore, uvedomovať si trestnoprávnu zodpovednosť v digitálnom priestore

- poznať princípy bezpečnej práce so súbormi a adresármi, poznať základné zásady zálohovania a šifrovania diskov
- poznať základné pojmy kryptológie, poznať rozdiely medzi asymetrickou a symetrickou kryptografiou, poznať koncept infraštruktúry verejného kľúča, rozdiel medzi digitálnym a elektronickým podpisom, rozoznať jednotlivé typy elektronických podpisov, vedieť použiť asymetrickú kryptografiu v praxi (podpisovanie a šifrovanie dokumentov a emailových správ)
- poznať spôsoby odhalenie krádeže digitálnej identity a falošnej digitálnej identity v digitálnej komunikácii,
- poznať pojem osobného údaju, koncept ochrany osobných údajov, základné zásady pri spracúvaní osobných údajov, práva dotknutých osôb, ovládať spôsoby ochrany súkromia a osobných údajov v digitálnom priestore (napr. na sociálnych sieťach)

Obsah a rozsah vzdelávacieho programu

Tematický celok	**Téma**	**Hodinová dotácia**
Bezpečnosť počítačovej siete	• Koncepcia informačnej bezpečnosti, základné pojmy a spôsob ich výučby, • Koncepcia výučby bezpečnosti počítačovej siete • Bezpečnosť pripojenia do počítačovej siete (LAN, wifi, mobilná sieť) • Nastavenie domáceho sieťového routra • 802.11 štandardy, kanál, kľúč, kryptografia, kryptoanalýza • WPA, kľúč, heslo • Virtuálne prostredie pre GNU/Linux, spustenie Rasbery Pi • Inštalácia a konfigurácia virtuálneho prostredia	**8 vh**

Tematický celok	Téma	Hodinová dotácia
Bezpečnosť operačného systému	• Koncepcia výučby bezpečnosti operačného systému • Heslá – spôsob vytvárania a ukladania hesiel, administrátor, používateľ s obmedzenými právami • Operačný systém - aktualizácia, inštalácia, firewall, konfigurácia, systémové záznamy • Škodlivé programy a ochrana voči nim, Ransomware • Súbory – šifrovanie a dešifrovanie, nastavenie oprávnení • nainštalovať, nastaviť a aktualizovať antivírusový program, vykonať celkovú kontrolu operačného systému	**8**
Bezpečnosť aplikácií	• Koncepcia výučby bezpečnosti aplikácií • Základné pojmy kryptológie • Bezpečná práca s dokumentami • Bezpečná práca s webom • Bezpečná komunikácia • Elektronická komunikácia so štátom • Práca s viacerými poštovými klientami: Mozilla Thunderbird, Enigmail, GPG, LibreOffice, MS Office	**8**
Bezpečnosť údajov a používateľa	• Koncepcia výučby bezpečnosti údajov a používateľa • Zálohovanie, obnova a likvidácia údajov • Súkromie, osobné údaje • Práva dotknutých osôb pri ochrane osobných údajov • Sociálne inžinierstvo – koncept a phishing • Kybernetická kriminalita – koncept, zodpovednosť, trestný čin, kyber-šikana, • Kybernetická kriminalita – počítačové trestné činy	**9**
Spolu		**33**

Materiálno technické zabezpečenie

Počítačová učebňa vybavená počítačovou technikou minimálne s takýmito technickými parametrami:

- každý žiak bude mať samostatné pracovisko (stôl, stoličku, počítač, monitor a príslušenstvo),
- učiteľ bude mať k dispozícii identické pracovisko ako žiak,
- všetky pracoviská budú zapojené do počítačovej siete s prístupom do Internetu,
- každé pracovisko bude obsahovať minimálne nasledujúci softvér: aktualizovaný operačný systém Microsoft Windows s antivírusovou ochranou, Microsoft Office, webové prehliadače Google Chrome, Mozilla Firefox a Internet Explorer v najnovších verziách , virtualizačné prostredie VirtualBox, príslušný softvér ku hardvéru.