REPUBLIKOVÁ ÚNIA RÚZ ZAMESTNÁVATEĽOV

VÝUČBA KYBERNETICKEJ BEZPEČNOSTI NA SOŠ

ANALÝZA

REPUBLIKOVÁ ÚNIA ZAMESTNÁVATEĽOV JE ČLENOM:

BUSINESSEUROPE

IOE

BUSINESSatOECD

VÝUČBA KYBERNETICKEJ BEZPEČNOSTI NA SOŠ:

VYTVORENIE PODMIENOK NA KOMPLEXNEJŠIU UPLATNITEĽNOSŤ ABSOLVENTOV STREDNÝCH ODBORNÝCH ŠKÔL V RÁMCI INOVAČNÝCH TRENDOV V OBLASTI KYBERNETICKEJ BEZPEČNOSTI

Štúdiu vypracoval kolektív autorov:

MGR. MAREK ZEMAN PHD. CRISC
DOC. ING. DAGMAR VIDRIKOVÁ, PHD.
ING. DANA JUHÁSOVÁ
MGR. JURAJ BADÁNI
ING. MIROSLAVA GUZLEJOVÁ
ING. JOZEF KRIVEK
MGR. RICHARD KIŠKOVÁČ, CISSP
ING. MÁRIO LELOVSKÝ
MARTIN MARTINKOVIČ
ING. JÁN LICHVÁR
JAKUB BUDINSKÝ

OBSAH

ZOZNAM TABULIEK

DÔVODOVÁ SPRÁVA

Predkladaný návrh obsahu vzdelávania vo vzťahu k prioritám a trendom v oblasti kybernetickej bezpečnosti vychádza z potreby riešiť problém zväčšujúceho sa nesúladu vzdelávacích výstupov škôl s potrebami praktického života a potrebami trhu práce vo viacerých sektoroch hospodárstva, najmä v informačných technológiách a súvisiacich službách[1]. Pálčivým problémom kybernetickej bezpečnosti je nedostatok disponibilných odborníkov. Na chýbajúce ľudské zdroje upozorňuje Európska komisia, Národný bezpečnostný úrad, Ministerstvo investícií, regionálneho rozvoja a informatizácie aj zamestnávateľské zväzy.

Existujúce študijné a učebné odbory pre stredné odborné školy (SOŠ) nedostatočne pokrývajú naliehavý trend digitálnej transformácie podnikov, organizácií a celej spoločnosti. Študijné odbory nie sú dostatočne pripravené na vzdelávanie a prípravu odborníkov v oblasti kybernetickej bezpečnosti. Jedná sa najmä o študijné odbory 25 Informačné a komunikačné technológie, ktoré nedokážu reagovať na zmeny na trhu práce.

Vzniká preto potreba vytvoriť nový alebo upraviť existujúci študijný odbor zabezpečujúci odborné vzdelávanie a prípravu žiakov na výkon povolania alebo odborných činností v oblasti kybernetickej bezpečnosti a prostredníctvom ktorého by získali potrebné vedomosti, schopnosti, zručnosti a kompetencie. Nižšie sa predkladajú relevantné argumenty na vytvorenie/úpravu vybraného študijného odboru.

Aktuálne globálne spoločenské a technologické výzvy prinášajú tlak na zmenu smerovania výchovy a prípravy novej generácie na budúce pracovné uplatnenie. Tieto výzvy prestupujú horizontálne celým spektrom verejných politík – od európskej úrovne, cez národné až po regionálne úrovne. Verejné politiky definujú (na európskej úrovni[2]), resp. stanovené priority preberajú (na národných/regionálnych úrovniach) a konkretizujú ich v strategických dokumentoch, aby sa postupne prejavili v celej spoločnosti a v každom sektore hospodárstva.

Poslanie tejto priority je potrebné chápať v širšom kontexte hlavných cieľov v oblasti digitalizácie na úrovni EÚ, ktoré sú zadefinované v dokumente Digitálny kompas 2030[3]. Misiou Digitálneho kompasu 2030 je digitálna transformácia v záujme konkurencieschopnosti a odolnosti Európy. Vízia do roku 2030 popisuje posilnenie postavenia občanov a podnikov, pričom digitálne ciele sú uvedené 4 kategóriách: 1) digitálne zručnosti obyvateľov, 2) bezpečná digitálna infraštruktúra, 3) digitálna transformácia podnikov a 4) digitalizácia verejných služieb. Cieľovým stavom je aktívne digitálne občianstvo. To všetko je vo veľkej miere podmienené dostatočnou úrovňou kybernetickej bezpečnosti, ktorú je nevyhnutné zabezpečiť nakoľko je nosným pilierom dôvery ako základného predpokladu digitálnej transformácie.

Časť aktivít pri napĺňaní Digitálneho kompasu 2030 zastrešuje Program Digitálna Európa (2021 – 2027)[4], ktorý je významným zdrojom financovania digitalizácie v EÚ (napr. financovaním siete európskych centier digitálnych inovácií[5]). Ďalším programom je Spájanie Európy (CEF Digital) 2021 – 2027[6]. Z pohľadu národných verejných politík je základným strategickým dokumentom Stratégia digitálnej transformácie Slovenska 2030[7] a z nej vyplývajúci Akčný plán digitálnej transformácie Slovenska na roky 2023 – 2026[8].

Z pohľadu prípravy a vzdelávania absolventov pre potreby trhu práce je digitálne vzdelávanie a jeho rozvoj na európskej úrovni popísané v Akčnom pláne digitálneho vzdelávania (2021 – 2027)[9] a na Slovensku sa tejto téme venuje Program informatizácie školstva do roku 2030[10] a k nemu príslušný aktuálny Akčný plán informatizácie a digitálnej transformácie vzdelávania v SR na obdobie 2021 – 2024[11], ako aj Akčný plán digitálnej transformácie Slovenska na roky 2023 – 2026[12] a ďalšie súvisiace dokumenty[13].

V neposlednom rade, dlhodobé zaostávanie Slovenska v oblasti napredovania v digitálnych cieľoch v rámci EÚ rieši Stratégia a akčný plán na zlepšenie postavenia Slovenska v indexe DESI do roku 2025[14], ktorá navrhovanými opatreniami vhodne dopĺňa vyššie uvedené strategické dokumenty a spoločne tak vytvárajú vhodné legislatívne prostredie na naštartovanie zmien v oblasti skvalitnenia slovenského odborného školstva.

EÚ sa intenzívne zameriava na posilnenie kybernetickej odolnosti, boj proti počítačovej kriminalite, ako aj na rozvoj kybernetickej diplomacie a obrany. Dôkazom týchto snáh je nová Stratégia kybernetickej bezpečnosti EÚ v digitálnej dekáde[15], ktorá bola predstavená v decembri 2020 Európskou komisiou.

Stratégia sa zameriava na tri hlavné oblasti: odolnosť, budovanie operačnej kapacity a podporu globálneho a otvoreného kybernetického priestoru. Tieto tri oblasti sú vzájomne prepojené a vytvárajú ucelený prístup k riešeniu kybernetických hrozieb. EÚ plánuje prijať rôzne opatrenia na dosiahnutie týchto cieľov, vrátane vytvorenia siete centier pre bezpečnostné operácie, zriadenia "Spoločnej kybernetickej jednotky" a posilnenia investícií do výskumu a inovácií. Dôležitou súčasťou stratégie je aj posun od reaktívneho k proaktívnemu prístupu, s dôrazom na včasnú detekciu hrozieb a prevenciu útokov.

EÚ však čelí v oblasti kybernetickej bezpečnosti mnohým výzvam, ako napríklad rastúca sofistikovanosť kybernetických útokov, rastúci počet pripojených zariadení a nedostatok kvalifikovaných pracovníkov. Rozdiely v úrovni kybernetickej bezpečnosti medzi členskými štátmi a rastúca hrozba štátnych kybernetických útokov predstavujú ďalšie prekážky. Na prekonanie týchto výziev je nevyhnutná úzka spolupráca medzi členskými štátmi, orgánmi EÚ a medzinárodnými partnermi.

Navrhovaný nový/upravovaný študijný odbor musí vychádzať z inovatívneho obsahu odborných a všeobecných predmetov, najmä musí adekvátne integrovať STEM predmety (science, technology, engineering, mathematics) do obsahu vzdelávania. Vyučovacie predmety fyzika, matematika a informatika sú kľúčové pre technické odbory. Formujú technické a prírodovedné myslenie a predurčujú tak úspech absolventa v ďalšom štúdiu alebo v praxi v odbore.

Problematika kybernetickej bezpečnosti, ktorá je z legislatívneho hľadiska upravená najmä tzv. smernicou NIS2[16]. Do štruktúry národných právnych predpisov je transformované prostredníctvom Zákona o kybernetickej bezpečnosti[17] ktorý komplexne upravuje oblasť kybernetickej a informačnej bezpečnosti, zavádza základné bezpečnostné požiadavky a opatrenia dôležité pre koordinovanú ochranu informačných, komunikačných a riadiacich systémov. Za účelom transformácie NIS2 v súčasnej dobe prebieha novelizácia uvedeného zákona. Zákon je doplnený viacerými vykonávacími predpismi vo forme vyhlášok. Pre vzdelávanie je dôležitá najmä Vyhláška Národného bezpečnostného úradu č. 492/2022 Z. z., ktorou sa ustanovujú znalostné štandardy v oblasti kybernetickej bezpečnosti[18].

Kybernetická bezpečnosť je ďalej zakotvená v strategických dokumentoch ako Stratégia kybernetickej bezpečnosti Slovenskej republiky na roky 2021 – 2025[19] a Akčný plán realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2021 až 2025[20].

V Akčnom pláne realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2021 až 2025 boli pre oblasť stredných odborných škôl stanovené úlohy uvedené v tabuľke č. 1.

Tabuľka č. 1 Úlohy definované pre oblasť stredných škôl

Kód úlohy	Úloha Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie
F.26	**Vzdelávanie a príprava kvalitných IT špecialistov na kybernetickú bezpečnosť** Vytvoriť koncept podpory odborného vzdelávania a v skupine odborov 25 IKT na stredných odborných školách v oblasti kybernetickej bezpečnosti	MŠVVaŠ SR	ŠIOV, stredné odborné školy a ich zriaďovatelia, RUZ	06/2022

F.27	Inovovať školské vzdelávacie programy a vytvoriť a overiť 10 vzorových školských vzdelávacích programov stredných odborných škôl so zapracovanými požiadavkami v oblasti kybernetickej bezpečnosti podľa aktuálneho vývoja a požiadaviek na trhu práce, v spolupráci so zamestnávateľmi súkromnej sféry a fakultami vysokých škôl technického zamerania	MŠVVaŠ SR	ŠIOV, stredné odborné školy a ich riaďovatelia, RUZ, súkromný sektor, vysoké školy	12/2022
F.28	Vybaviť stredné školy vzdelávajúce v skupine odborov 25 IKT technológiou a laboratóriami pre podporu výuky predmetov zameraných na kybernetickú bezpečnosť	MŠVVaŠ SR	stredné odborné školy a ich zriaďovatelia	06/2024
F.29	Revidovať a navýšiť normatív pre udržateľnosť kvality vzdelávania v skupine odborov 25 IKT so zameraním sa na kybernetickú bezpečnosť	MŠVVaŠ SR	ŠIOV, stredné odborné školy a ich zriaďovatelia	12/2022
F.30	Podporiť vypracovanie dvoch nových odborov na stupni vzdelávania „Q“ pre prvý stupeň terciárneho vzdelávania (ISCED B5) pomaturitného resp. špecializačného vzdelávania vrátane ich profilácie na kybernetickú bezpečnosť	MŠVVaŠ SR	ŠIOV, stredné odborné školy a ich zriaďovatelia, RUZ	01/2023
F.31	Aktualizovať a doplniť technologické vybavenie programu Sieťových akadémií na Slovensku pre podporu vzdelávania špecialistov na vysokých a stredných školách v oblasti kybernetickej bezpečnosti.	MŠVVaŠ SR	Vysoké školy, stredné školy, tretí sektor	01/2024
F.36	Vytvoriť legislatívne prostredie, naviazané na potreby zamestnávateľov v oblasti zvyšovania zručností zamestnancov pre využívanie prvého stupňa terciárneho vzdelávania na stredných odborných školách v prepojení na potreby praxe a možnosti pokračovania vo vysokoškolskom vzdelávaní, prípadne externej formy štúdia zamestnanca na vysokých školách v študijných odboroch a programoch v oblasti kybernetickej bezpečnosti a podpora vzdelávania dospelých v kurzoch v oblasti kybernetickej bezpečnosti	MŠVVaŠ SR	MPSVaR, Rada zamestnávateľov pre OVP	12/2022
F.37	Posilniť popularizáciu stredoškolského i vysokoškolského štúdia technických a prírodovedných odborov (STEM) a kybernetickej bezpečnosti	MŠVVaŠ SR	MPSVaR SR, Zamestnávateľské zväzy, Rada zamestnávateľov pre OVP, samosprávne kraje	12/2022
F.38	Podporovať regionálne nadpodnikové centrá praxe a inovácií pre zapájanie špecialistov kybernetickej bezpečnosti zo súkromného sektora a doktorandov vysokých škôl do odborného vzdelávania a prípravy	MŠVVaŠ SR		12/2022

Je potrebné skonštatovať, že z uvedených úloh akčného plánu, špecificky tých, ktoré sa týkajú stredných odborných škôl sa nepodarila zrealizovať do súčasnej doby žiadna v plánovanom rozsahu.

Z pohľadu trhu a možného dopytu po absolventoch študijného odboru zameraného na kybernetickú bezpečnosť vyplýva, že v rámci SR je dopyt po odborníkoch na kybernetickú bezpečnosť enormný. Podľa analýzy[21] Kompetenčného a certifikačného centra kybernetickej bezpečnosti z konca roka 2023 chýba na Slovensku približne 19 234 rôznych špecialistov v oblasti kybernetickej bezpečnosti.

V zmysle vyššie citovanej Vyhlášky NBÚ ktorou sa ustanovujú znalostné štandardy v oblasti kybernetickej bezpečnosti a pozícia Špecialista kybernetickej bezpečnosti javí ako najvhodnejšia na prípravu žiakov stredných odborných škôl.

Rola špecialistu kybernetickej bezpečnosti je najviac univerzálna pre vzdelávanie na stredných odborných školách z niekoľkých dôvodov. Kybernetická bezpečnosť je dynamicky sa rozvíjajúca oblasť s vysokým dopytom po kvalifikovaných odborníkoch. To znamená, že absolventi stredných odborných škôl so zameraním na kybernetickú bezpečnosť majú vynikajúce vyhliadky na zamestnanie a kariérny rast. Rola špecialistu kybernetickej bezpečnosti zahŕňa širokú škálu technických zručností a znalostí, ktoré sú uplatniteľné v rôznych odvetviach a organizáciách. To študentom umožňuje získať ucelený súbor kompetencií, ktoré im otvoria dvere k rôznym profesijným príležitostiam.

Obdobná pozícia ako špecialista kybernetickej bezpečnosti je formálne zavedená aj v Národnej sústave kvalifikácií (NSK) s názvom Špecialista informačnej bezpečnosti pod kódom U2529001-01387 a SK ISCO-08 2529001 Špecialista bezpečnosti IT[22], avšak do budúcnosti bude potrebná aj inovácia tejto kvalifikácie zjednotením pojmov informačná a kybernetická bezpečnosť.

Pozícia špecialistu kybernetickej bezpečnosti je taktiež zavedená v registri zamestnaní pod kódom 17928/2[23], kde je však odporúčané vysokoškolské vzdelanie II. stupňa.

V zákone o kybernetickej bezpečnosti sú zakotvené iba dve roly v kybernetickej bezpečnosti, ktorých činnosť by mala byť pre prevádzkovateľov základnej služby záväzná a ktoré by mali spĺňať stanovený znalostný štandard:

- audítor kybernetickej bezpečnosti - podľa § 29 ods. 3 Zákona o kybernetickej bezpečnosti audit kybernetickej bezpečnosti vykonáva certifikovaný audítor kybernetickej bezpečnosti, ktorým je fyzická osoba, spoločník, štatutárny orgán alebo zamestnanec právnickej osoby; činnosť audítora kybernetickej bezpečnosti upravuje vyhláška č. 493/2022 Z. z. o audite kybernetickej bezpečnosti,
- manažér kybernetickej bezpečnosti - v zmysle § 20 ods. 4 Zákona o kybernetickej bezpečnosti bezpečnostné opatrenia musia zahŕňať najmenej určenie manažéra kybernetickej bezpečnosti.

Ďalšou rolou, ktorá je významná z pohľadu požiadaviek trhu v súvislosti s platnou legislatívou je Manažér kybernetickej bezpečnosti. Pozícia manažéra kybernetickej bezpečnosti sa od špecialistu líši v niekoľkých kľúčových aspektoch. Manažér je zodpovedný za strategické plánovanie a riadenie kybernetickej bezpečnosti v organizácii. To zahŕňa tvorbu bezpečnostných politík, riadenie rizík, koordináciu tímu špecialistov a komunikáciu s vedením spoločnosti. Manažér musí mať hlbšie znalosti o kybernetických hrozbách a trendoch, ale aj silné komunikačné a strategické zručnosti. Z týchto dôvodov je manažér kybernetickej bezpečnosti skôr nadstavbou pre špecialistov a jeho pozícia nie je úplne vhodná pre stredné odborné školy. Vzdelávacie programy na stredných školách sa zameriavajú na získavanie praktických zručností a základných teoretických vedomostí, ktoré sú nevyhnutné pre výkon roly špecialistu. Stredná odborná škola pripravuje študentov na to, aby sa stali kvalifikovanými špecialistami v oblasti kybernetickej bezpečnosti, ktorí môžu po absolvovaní školy a získaní praxe ďalej napredovať a časom sa vypracovať aj na manažérske pozície. Okrem toho je pre výkon tejto pozície vyžadovaná v zmysle zákona certifikácia v zmysle certifikačnej schémy overovania odbornej spôsobilosti manažéra kybernetickej bezpečnosti[24].

Na základe vyššie uvedených dôvodov bola pre návrh nového, alebo inováciu študijného odboru vybraná pre absolventov študijného odboru ako cieľová pozícia špecialista kybernetickej bezpečnosti.

PRÍPRAVA A TVORBA VÝSTUPU

Vypracovanie návrhu obsahu vzdelávania pozostávalo z nasledovných častí:

- Vytvorenie pracovnej skupiny zloženej zo zástupcov odborného vzdelávania a prípravy a expertov v oblasti kybernetickej bezpečnosti.
- Analýza existujúcich súvisiacich štátnych vzdelávacích programov, rámcových učebných plánov zo skupiny odborov 25 a 26. Spracovanie dôvodovej správy z aktuálneho stavu problematiky ľudských zdrojov v oblasti kybernetickej bezpečnosti.
- Vypracovanie obsahu inovovaného študijného odboru v oblasti kybernetickej bezpečnosti.

Vytvorenie expertnej pracovnej skupiny a predpokladaný harmonogram prác:

S cieľom posúdiť skupiny odborov 25 Informačné a komunikačné technológie, prípadne 26 Elektrotechnika a vypracovania návrhu obsahu študijného odboru so zameraním na kybernetickú bezpečnosť bola vytvorená expertná pracovná skupina zložená zo zástupcov odborného vzdelávania a prípravy (Stredná priemyselná škola elektrotechnická Jozefa Murgaša Banská Bystrica), dlhoročných profesionálov v oblasti kybernetickej bezpečnosti, členov Sektorovej rady pre informačné technológie a telekomunikácie a zástupcov stavovských a profesijných organizácií. Členmi pracovnej skupiny boli nasledujúci odborníci zastupujúci vybrané inštitúcie:

- Mgr. Marek Zeman Phd. CRISC (Tatrabanka)
- Ing. Kamil Kordík (SPŠJM Banská Bystrica)
- doc. Ing. Dagmar Vidriková, PhD. (Accreditus s.r.o.)
- Ing. Dana Juhásová (SPŠJM Banská Bystrica)
- Mgr. Juraj Badáni (SPŠJM Banská Bystrica)
- Ing. Miroslava Guzlejová (SPŠJM Banská Bystrica)
- Ing. Jozef Krivek (SPŠJM Banská Bystrica)
- Mgr. Richard Kiškováč, CISSP (Elkan s.r.o.)
- Ing. Mário Lelovský (Republiková únia zamestnávateľov)
- Martin Martinkovič (Republiková únia zamestnávateľov)
- Ing. Ján Lichvár (Cluster Kybernetickej Bezpečnosti)
- Jakub Budinský (CoolPeople Technology)

V rámci spracovanie štúdie bol oslovený aj zástupca Štátneho inštitútu odborného vzdelávania (ďalej len „ŠIOV"), ktorý sa však odmietol zúčastniť na jej vypracovaní nakoľko sa nestotožnil so závermi komparatívnej analýzy vykonanej odborníkmi na kybernetickú bezpečnosť, ktorá vychádza z požiadaviek praxe. Do budúcna bude pre zjednotenie odborných hľadísk potrebná hlbšia odborná diskusia so zástupcami ŠIOV.

Členovia pracovnej skupiny spolupracovali formou osobných stretnutí ako aj prostredníctvom online komunikačných nástrojov (MS TEAMS), medzi členmi prebiehala mailová a telefonická komunikácia pod vedením realizačného tímu.

Celkové práce na vypracovaní návrhu obsahu vzdelávania boli naplánované na sedem pracovných týždňov (november – december 2024). Harmonogram prác zahŕňal spracovanie návrhu obsahu vzdelávania v oblasti kybernetickej bezpečnosti. Na základe analýzy relevantných študijných odborov bol obsah spracovaný formou inovácie študijného odboru 2561 M Informačné a sieťové technológie. Harmonogram prác bol nasledovný:

Tabuľka č. 2 Harmonogram tvorby návrhu obsahu vzdelávania

Harmonogram	25.–29. 11.	2.–6. 12.	9.–10. 12.	10.–11. 12.	12.–13. 12.
Uvedenie do problematiky a vstupná analýza aktuálneho stavu	x				
Analýza existujúcich súvisiacich štátnych vzdelávacích programov, rámcových učebných plánov zo skupiny odborov 25 a 26	x	x			
Popis profilu absolventa, definovanie obsahu a odporúčaní na vznik, resp. inováciu štátneho vzdelávacieho programu		x	x		
Identifikácia príležitostí vzdelávania (škôl a zamestnávateľov) v oblasti kybernetickej bezpečnosti.		x	x	x	
Analýza potenciálu uplatnenia absolventov a identifikácia možných cieľových skupín žiakov a rodičov pre oblasť štúdia kybernetickej bezpečnosti		x	x	x	
Pripomienkovanie spracovaného dokumentu pre oblasť inteligentných zariadení budov, domácností a miest			x	x	x
Finalizácia dokumentu v štruktúre štátneho vzdelávacieho programu stanoveného Štátnym inštitútom odborného vzdelávania				x	x

Zdroj: Realizačný tím

KOMPARATÍVNA ŠTÚDIA ZAVEDENIA ODBORU KYBERNETICKÁ BEZPEČNOSŤ

V rámci komparatívnej analýzy boli porovnané existujúce súvisiace štátne vzdelávacie programy rámcové učebné plány zo skupiny odborov 25 a 26. Analýza bola zameraná na zistenie úrovne relevancie pre oblasť kybernetickej bezpečnosti. V uvedených vzdelávacích programoch boli identifikované súvislosti aj rozdiely. Oba typy odborov, hoci sa primárne nezameriavajú na kybernetickú bezpečnosť avšak obsahujú prvky a témy relevantné pre túto oblasť.

Skupina 25 Informačné a komunikačné technológie sa vyznačuje širším záberom, zahŕňajúc programovanie, sieťové technológie, operačné systémy a databázy. V kontexte kybernetickej bezpečnosti sú tieto znalosti kľúčové pre pochopenie fungovania systémov, identifikáciu zraniteľností a implementáciu bezpečnostných opatrení. Odbory ako v skupine 25 priamo obsahujú moduly venované základom kybernetickej bezpečnosti, ale ich hĺbka a rozsah sú obmedzené. Chýbajú špecializované predmety, ktoré by detailnejšie vysvetľovali problematiku kybernetickej bezpečnosti a jej praktických aspektov (kybernetické útoky, ich prevencia a detekcia, etický hacking, kryptografia, forenzná analýza).

V rámci skupiny 25 boli porovnané vzdelávacie odbory 2561 M Informačné a sieťové technológie, odbor 2559 M Inteligentné technológie a odbor 2573 M Programovanie digitálnych technológií s cieľom zhodnotenia prieniku ich obsahu s požiadavkami v oblasti kybernetickej bezpečnosti.

Odbor 2561 M Informačné a sieťové technológie sa zameriava najmä na hardvér, softvér, počítačové siete a programovanie. V kontexte kybernetickej bezpečnosti poskytuje absolventom dobrý základ pre pochopenie fungovania informačných systémov, identifikáciu zraniteľností a implementáciu bezpečnostných opatrení. Študenti sa učia o operačných systémoch, sieťových protokoloch, programovaní a databázach, čo sú všetko dôležité znalosti pre oblasť kybernetickej bezpečnosti.

Odbor 2559 M Inteligentné technológie je novším odborom zameraným na moderné technológie ako internet vecí (IoT), umelá inteligencia (AI) a analýza dát. Z pohľadu kybernetickej bezpečnosti je dôležitý najmä dôraz na IoT, ktoré prináša nové bezpečnostné výzvy. Absolventi tohto odboru majú potenciál uplatniť sa v oblasti zabezpečenia IoT zariadení a sietí. Avšak, odbor sa venuje kybernetickej bezpečnosti len okrajovo, v kontexte bezpečnosti IoT. Z pohľadu kybernetickej bezpečnosti odbor 2561 M obsahuje samostatný modul venovaný základom kybernetickej bezpečnosti a odbor 2559 M sa venuje kybernetickej bezpečnosti obmedzene, iba v kontexte IoT.

Odbor 2573 M Programovanie digitálnych technológií je v súčasnosti odborom v experimentálnom overovaní. Odbor je zameraný na programovanie širokého spektra digitálnych technológií s využitím moderných vývojových nástrojov, postupov a jazykov. V rámci študijného odboru programovanie digitálnych technológií je umožnené žiakom odborne sa zamerať na programovanie internetových aplikácií (používateľské rozhranie a dizajn – frontend a administrácia – backend), programovanie hier so silným zastúpením techník pre virtuálnu realitu, 3D zobrazovanie, či prvky umelej inteligencie a na programovanie komerčných podnikových aplikácií, napr. ERP systémov.

Skupina 26 Elektrotechnika sa zameriava na hardvér, elektroniku a elektrotechnické systémy. Z pohľadu kybernetickej bezpečnosti sú tieto vedomosti dôležité pre pochopenie fungovania hardvérových komponentov, sietí a komunikačných systémov, ktoré môžu byť cieľom kybernetických útokov. Odbory ako 2682 K mechanik počítačových sietí sa venujú konfigurácii a správe sietí, čo je relevantné pre sieťovú bezpečnosť, ale opäť chýba širší kontext kybernetickej bezpečnosti.

Porovnaním skupín bolo zistené, že skupina 25 sa zameriava na viac na softvér, operačné systémy a siete, zatiaľ čo skupina 26 viac na hardvér a elektroniku. Skupina 25 poskytuje širší prehľad o IT technológiách, ktoré sú skupina 26 sa viac špecializuje na elektrotechniku. V skupine 25 sú základy kybernetickej bezpečnosti priamo zahrnuté v niektorých odboroch, v skupine 26 sú tieto vedomosti skôr implicitné a vyplývajú zo znalostí o hardvéri a sieťach.

Na základe porovnania študijných odborov 25 a 26 bolo je možné konštatovať, že z pohľadu sledovaných cieľov tejto analýzy majú k oblasti kybernetickej bezpečnosti bližšie študijné odbory 25, ktoré už v súčasnej dobe poskytujú svojim študentom širšiu škálu potrebných vedomostí.

Ďalej sme v rámci analýzy sme pracovali s týmito možnými alternatívami návrhu:

- Inovácia jedného existujúceho odboru, kde do úvahy prichádzajú

  2561 M Informačné a sieťové technológie

  2559 M Inteligentné technológie, odbor v experimente

  2573 M Programovanie digitálnych technológií

- Návrh nového odboru v skupine odborov vzdelávania 25
- Návrh pomaturitného odboru

Inovácia existujúceho študijného odboru 2561 M Informačné a sieťové technológie

Jednou z možností je inovovať už existujúci študijný odbor 2561 M Informačné a sieťové technológie. Tento študijný odbor bol v experimentálnom overovaní od roku 2008 a po jeho overení je ponúknutý v sieti študijných odborov. Jedná sa o stabilný študijný odbor, ktorý ponúka úplné stredné vzdelanie ISCED 3A ukončené maturitnou skúškou.

Absolvent študijného odboru Informačné a sieťové technológie je kvalifikovaný zamestnanec schopný samostatne vykonávať práce pri projektovaní, konštrukcii, výrobe, montáži, ako aj v prevádzke a údržbe zariadení, využívajúcich moderné informačné a komunikačné technológie (IKT).

Pre kvalifikované vykonávanie uvedených činností absolvent štúdia získava široký odborný profil. Po nástupnej praxi je pripravený na výkon technika konštrukčného, technologického, montážneho a prevádzkového charakteru v oblastiach IKT, ale aj na ďalšie funkcie v odborných útvaroch. Odbornou praxou a ďalším štúdiom si zvyšuje svoje zručnosti a vedomosti, čím si zvyšuje svoju odbornú kvalifikáciu. Absolvent študijného odboru Informačné a sieťové technológie má na základe svojej prípravy všetky predpoklady pre zvládnutie vysokoškolského štúdia.

Významnou súčasťou tohto študijného odboru na mnohých stredných školách je integrácia na Sieťový akademický program – NetAcad (https://www.netacad.com/), spoločnosti CISCO (CISCO Academy), ktorá umožňuje úzku prepojenosť na niektoré odborné predmety. Zameriava sa najmä na sieťové technológie ich prevádzku ako aj bezpečnosť. Po ukončení tohto programu a úspešnom absolvovaní externej skúšky majú absolventi možnosť získať medzinárodne uznávané priemyselné certifikáty (napr. CNA -Cisco Certified Network Associate).

Odborné vzdelávanie by pozostávalo z praktickej a teoretickej časti. V rámci odboru by bolo možné vyučovať odborné predmety, ktoré sú neoddeliteľnou súčasťou pochopenia a praktickej realizácie v oblasti kybernetickej bezpečnosti, pretože vysvetľujú fungovanie informačných a komunikačných technológií a to najmä:

- Operačné systémy
- Sieťové technológie
- Serverové technológie
- Počítačová architektúra

V čase vzniku tohto odboru nebola oblasť kybernetickej bezpečnosti v praxi natoľko exponovaná aby bol vytvorený konkrétny predmet s týmto názvom. V súčasnosti je však nevyhnutné kybernetickú bezpečnosť vhodne zapracovať aj do tohto odboru. Táto oblasť sa stáva kľúčovou a absolventi odboru sa s ňou budú často v praxi stretávať. Príkladom z praxe je Stredná priemyselná škola Jozefa Murgaša v Banskej Bystrici, ktorá rozšírením obsahového štandardu odboru IST pridala obsah zameraný na kybernetickú bezpečnosť s názvom predmetu Kybernetická bezpečnosť.

Navrhovaný odborný predmet Kybernetická bezpečnosť rozširuje vedomosti predmetov Sieťové technológie, Operačné systémy, Serverové technológie a Programovanie. Cieľom vyučovacieho predmetu je poskytnúť žiakom súbor vedomostí, zručností a kompetencií v oblasti kybernetickej bezpečnosti, jej zloženie, vplyv, bezpečnosť, finančné náklady a legislatívne kompetencie v Slovenskej republike. Zároveň majú získať praktické zručnosti a kompetencie obsahujúce princípy kybernetickej bezpečnosti a technológií v praxi, implementáciu bezpečnostných technológií, prostriedkov a zariadení. Naučiť sa identifikovať problémy a efektívne ich riešiť, rozvíjať základné komunikačné zručnosti a spoluprácu pri riešení problémov.

Pri výbere učiva je potrebné prihliadať hlavne na využiteľnosť poznatkov v praxi. Obsahom predmetu môžu byť aj priamo kurzy v rámci Cisco Academy ako je Cyber Opps alebo Ethical Hacker, ktoré sa venujú tejto oblasti.

Ďalšou možnosťou v odbore 2561 M Informačné a sieťové technológie by bola jeho inovácia formou zamerania s využitím voliteľných predmetov pre 3. a 4. ročník. To by znamenalo, že absolvent by mal po absolvovaní 2. ročníka možnosť výberu zamerania. Najvhodnejším by bola nasledovná skladba zameraní:

- Špecialista informačných technológií
- Špecialista kybernetickej bezpečnosti

Absolvent zamerania Špecialista informačných technológií by sa špecializoval hlavne na všeobecnú správu serverov, sietí, programovanie, databázové a webové aplikácie. Absolvent zamerania Špecialista kybernetickej bezpečnosti by sa špecializoval na kybernetickú bezpečnosť serverov, sietí, koncových bodov, webových aplikácií, kryptografiu, programovanie, právnu výchovu a manažment bezpečnostných rizík. Obsahová štruktúra oboch zameraní by bola v prvých dvoch ročníkoch rovnaká, čo by kopírovalo pôvodný obsah tohto odboru. Tento prístup korešponduje aj so súčasnými trendami v školstve.

Inovácia existujúceho odboru je flexibilnejšia a umožňuje rýchlejšie zapracovať nové poznatky a trendy do výučby. Naviac skladba a obsah odborných predmetov v prvých dvoch ročníkoch umožňuje vhodne nadviazať na oblasť kybernetickej bezpečnosti.

Naopak nevýhodu tohto riešenia vidíme v obmedzenom rozsahu pre implementáciu zmien do školského vzdelávacieho programu (ŠkVP). Inovácie môžu byť zavedené len v rozsahu disponibilných hodín a predefinovaním obsahu niektorých odborných predmetov. Zmenu by bolo možné aplikovať od ďalšieho školského roka začínajúc prvým ročníkom, čiže by trvalo štyri roky, kým by bolo možné zavedenú inováciu overiť. Napriek tomu je toto riešenie však relatívne najrýchlejšie pre zavedenie do praxe.

Je však potrebné dodať, že odbor Informačné a sieťové technológie je v súčasnosti ponúkaný aj na školách, ktorým chýba materiálovo-technické vybavenie, ľudské zdroje alebo majú primárne iné zameranie ich možností štúdia a výsledkom je menej kvalitná výučba. Záujem o odbor kontinuálne klesá aj tým, že sa začínajú ponúkať iné odbory v skupine odborov 25. Preto by navrhovaná inovácia mohla pomôcť aj jeho oživeniu.

Inovácia existujúceho študijného odboru 2559 M Inteligentné technológie

Študijný odbor 2559 M Inteligentné technológie bol vypracovaný na základe požiadavky Republikovej únie zamestnávateľov podľa potrieb digitálnej transformácie a Industry 4.0 a tohto času je stále v experimente.

Absolvent študijného odboru inteligentné technológie je kvalifikovaný odborný pracovník, ktorý má vedomosti a zručnosti z oblasti informačných technológií, programovania, počítačových sietí, smart technológií, internetu vecí - IoT, databázových systémov, kybernetickej bezpečnosti, robotiky, 3D technológií, virtuálnej reality, z aplikovania prvkov umelej inteligencie v rôznych oblastiach, serverových a cloudových technológií, grafiky, základov elektroniky, optimalizácie riadenia procesov a problematiky súvisiacej s digitálnou firmou. Absolvent dokáže vytvoriť vývojový diagram postupnosti tvorby programu a programovať vo viacerých programovacích jazykoch.

Dokáže vytvárať dynamické webové stránky s prepojením na databázový systém, rozumie pojmu „Big data“ a ovláda spôsoby monitorovania a analýzy dát, dokáže pracovať s databázami. Má dobré vedomosti z matematiky (potreba matematiky z dôvodu logického myslenia, tvorby algoritmov a programovania). Je schopný využívať mäkké zručnosti v prezentovaní a vystupovaní.

Súčasťou tohto študijného odboru na mnohých stredných školách je tiež integrácia na Sieťový akademický program – NetAcad, spoločnosti CISCO s úzkou prepojenosťou na niektoré predmety. Odborné vzdelávanie pozostáva z praktickej a teoretickej časti.

Ide o nový, moderný odbor o ktorý je zo strany žiakov veľký záujem. Má zaujímavú skladbu predmetov, kde sa žiaci učia nové digitálne technológie a nové trendy s veľmi dobrým obsahom. Nosnými sú predmety ako IoT, robotika, SMART technológie, dizajn digitálnych médií, 3D technológie, umelá inteligencia. Má už v sebe zakomponovaný predmet kybernetická bezpečnosť i keď s menšou časovou dotáciou. Bolo by vhodné im zakomponovať oblasť legislatívy a práva. Odbor je v ponuke už šiestym rokom a spätnou väzbou bolo zistené, že chýbajú aj predmety z oblasti virtualizácie a operačných systémov.

Tento odbor považujeme za nevhodný pre inováciu pre oblasť kybernetickej bezpečnosti. Dôvodom je najmä nie úplne adekvátna skladba odborných predmetov. V prípade inovácie by sa vyžadovalo doplnenie skladby odborných predmetov na úroveň študijného odboru 2561 M Informačné a sieťové technológie. Z tohto dôvodu je výhodnejšie priamo inovovať študijný odbor 2561 M Informačné a sieťové technológie.

Inovácia existujúceho študijného odboru 2573 M Programovanie digitálnych technológií

Odbor je v súčasnosti odborom v experimentálnom overovaní. Experimentálnym overovaním bola od 1. septembra 2020 poverená Stredná odborná škola informačných technológií, Ostrovského 1, Košice a rozšírením projektu experimentálneho overovania aj Stredná odborná škola elektrotechnická, Zochova 9, Bratislava. Od 1. septembra 2021 pristúpila do experimentálneho overovania aj Stredná odborná škola elektrotechnická, Hálova 16, Bratislava. Perspektívne bude úspešne ukončené experimentálne overovanie 31.8.2026 tak, aby sa od 1.9.2026 dostal do vyhlášky o sústave odborov vzdelávania. Odbor umožňuje absolventom získať úplné stredné odborné vzdelanie v oblasti odborov informačno-komunikačných technológií. Absolventi nadobudnú potrebné základné vedomosti a zručnosti v odbornom vzdelávaní i praktickej príprave, od tretieho ročníka sa odborne profilujú na: programovanie internetových aplikácií (so zameraním na programovanie používateľského rozhrania a dizajnu front-end alebo programátori administrácie a celkovej funkcionality back-end) a programovanie hier (so zameraním na virtuálnu realitu, 3D zobrazovanie, základy umelej inteligencie). Odbor je tiež špecificky zameraný na základy grafického dizajnu, skriptovacie jazyky, testovanie, herný dizajn, procedurálne jazyky.

Z hľadiska odbornej praxe v oblasti kybernetickej bezpečnosti je profilovanie absolventov v tomto odbore nevhodné pre oblasť kybernetickej bezpečnosti. Profil programátora a špecialistu kybernetickej bezpečnosti sa v praxi významne odlišujú. Pre oba profily je vyžadované odlišné zameranie, zručnosti, schopnosti a najmä požadovaný spôsob myslenia. Pre porovnanie uvádzame základné charakteristiky a odlišnosti uvedených profilov:

- Programátor – je zameraný na tvorbu programov, k čomu potrebuje vynikajúce ovládanie programovacích jazykov, algoritmov a dátových štruktúr. Vyžaduje sa od neho kreatívne myslenie, inovácie, zameranie na funkčnosť a biznis aktivity čo je v mnohých prípadoch v rozpore s kybernetickou bezpečnosťou.
- Špecialista na kybernetickú bezpečnosť – je zameraný na identifikáciu bezpečnostných rizík, návrh a prevádzku bezpečnostných opatrení, potrebuje hlboké znalosti operačných systémov, serverov, sietí, no najmä poznať hackerské techniky a taktiky. Vyžaduje sa od neho konzervatívne a kritické myslenie, ostražitosť, predvídavosť čo má za následok skôr obmedzovanie funkcionalít riešení či okliešťovanie biznis aktivít.

Z vyššie uvedených dôvodov ako aj na základe skúseností z praxe považujeme uvedený odbor za nevhodný na inováciu pre oblasť kybernetickej bezpečnosti. Bolo by nežiadúce meniť profil absolventa z programátora na špecialistu kybernetickej bezpečnosti. Tieto profily sú v praxi značne odlišné a čiastočne protichodné. Výsledkom by bola degradácia jedného alebo druhého profilu čo by viedlo k celkovému zníženiu odbornej pripravenosti absolventov. Vzhľadom na značný nedostatok programátorov bude vhodnejšie v rámci odboru plne rozvíjať profil programátora a takto reagovať na potreby trhu práce. Zachovaním profilu je možné odbor obohatiť o témy ako bezpečnosť aplikácií, bezpečný vývoj softvéru, avšak tieto oblasti pokrývajú odhadom iba 5 % z celkovej problematiky kybernetickej bezpečnosti.

Vytvorenie nového študijného odboru skupiny študijných odborov 25 Informačné a komunikačné technológie

Rastúca potreba riešiť kritické výzvy digitálnej transformácie a narastajúce hrozby v oblasti informačnej bezpečnosti dáva dobré predpoklady aj na vznik nového študijného odboru so zameraním na kybernetickú bezpečnosť. Kybernetická bezpečnosť sa stáva extrémne dôležitou z hľadiska hospodárskeho a spoločenského rozvoja, pričom súčasné vzdelávacie programy bez vykonania radikálnych zmien nedostatočne reflektujú na potrebu prípravy kvalifikovaných odborníkov v tejto oblasti.

Ako je uvedené v predchádzajúcej časti dokumentu, existujúce študijné a príp. aj učebné odbory pre stredné odborné školy pokrývajú iba čiastkové aspekty kybernetickej bezpečnosti. V skupine vzdelávania 25 (Informačné a komunikačné technológie) príp. 26 (Elektrotechnika) chýbajú jednotné programy, ktoré by poskytovali absolventom komplexné vedomosti a zručnosti potrebné na zabezpečenie ochrany dát, systémov a infraštruktúry pred kybernetickými hrozbami.

Z uvedených dôvodov by bolo najvýhodnejšie vytvorenie nového študijného odboru v skupine 25 zameraného výhradne iba na kybernetickú bezpečnosť. Tento odbor by poskytoval medziodborové kompetencie, ktoré spájajú poznatky z informatiky, elektrotechniky, práva, manažmentu rizík a psychológie. Absolventi by boli lepšie pripravení na požiadavky trhu práce a mohli by sa rýchlejšie uplatniť v praxi. Nový odbor by mohol prilákať viac študentov so záujmom o kybernetickú bezpečnosť.

Nový študijný obor by umožňoval poskytnúť viac vyučovacích hodín a teda aj viac času pre výučbu špecifických oblastí a tém kybernetickej bezpečnosti. Nebol by obmedzený iba na rozsah disponibilných hodín ako prípade inovácie odboru 2561 M Informačné a sieťové technológie. Je však otázne o aké navýšenie počtu vyučovacích hodín by sa jednalo nakoľko je nevyhnutné, aby jeho absolventi disponovali všeobecnými znalosťami fungovania IKT technológií a to najmä serverov, sietí, operačných systémov, programovania, databázových a webových aplikácií. Tieto oblasti sú doménou práve odboru 2561 M Informačné a sieťové technológie. Nový odbor by tak mohol viesť k duplicite prípadne neefektívnemu využitiu zdrojov.

Významnou nevýhodou je aj časová náročnosť zavedenia nového študijného odboru. Proces zavedenia nového študijného odboru je komplexný a pozostáva z niekoľkých štádií, ktoré si vyžadujú čas a koordináciu medzi rôznymi zainteresovanými stranami. Celkovo môže proces zavedenia nového študijného odboru trvať 3 až 5 rokov a jeho overovanie v experimentálnej fáze minimálne 4 roky. Znamená to, že jeho uvedenie do praxe a uvedenie nových absolventov na trh práce môže trvať najmenej 5 až 9 rokov. Počas tejto doby sa však oblasť kybernetickej bezpečnosti neustále vyvíja, vznikajú nové hrozby a technológie. To znamená, že študijný program, ktorý bol navrhnutý pred niekoľkými rokmi, nemusí byť v čase spustenia výučby už aktuálny. Zavedenie nového odboru teda predstavuje riziko, že absolventi nebudú mať dostatočné vedomosti a zručnosti na to, aby sa úspešne uplatnili na trhu práce. Navyše, časová náročnosť celého procesu môže viesť k oneskoreniu v príprave kvalifikovaných odborníkov v oblasti kybernetickej bezpečnosti.

Vzhľadom na dynamický charakter kybernetickej bezpečnosti je preto efektívnejšie zamerať sa na inováciu existujúcich študijných odborov, ktoré umožňujú flexibilnejšie reagovať na meniace sa potreby a trendy.

Pomaturitné štúdium zamerané na kybernetickú bezpečnosť

Vzdelávanie formou pomaturitného štúdia by umožňovalo získať kvalifikáciu ukončenú maturitnou skúškou, alebo doplniť a rozšíriť si kvalifikáciu nadobudnutú na strednej škole, ktorej zameranie nekorešpondovalo s kvalifikačnými požiadavkami na pozíciu riadiaceho pracovníka kybernetickej bezpečnosti.

Zavedenie študijného odboru zameraného na kybernetickú bezpečnosť formou pomaturitného štúdia by síce mohlo priniesť určité výhody, ako napríklad rýchlejšiu prípravu absolventov pre prax, avšak z pohľadu časovej náročnosti a dynamického vývoja v oblasti kybernetickej bezpečnosti by to nebolo najvhodnejšie riešenie. Hlavným problémom je obmedzený rozsah učiva, ktorý je možné pokryť v rámci jednoročného, alebo dvojročného štúdia. Kybernetická bezpečnosť je komplexná oblasť, ktorá si vyžaduje hlbšie znalosti z rôznych oblastí IKT technológií. V rámci jednoročného štúdia by nebolo možné dostatočne prehĺbiť všetky tieto oblasti a poskytnúť študentom komplexný prehľad o problematike kybernetickej bezpečnosti. Absolventi by tak mohli mať medzery vo vedomostiach, ktoré by im bránili v úspešnom uplatnení sa v praxi.

Pomaturitné štúdium kybernetickej bezpečnosti by mohlo byť koncipované ako jedno až dvojročné, v závislosti od hĺbky a rozsahu učebnej látky. Štúdium by mohlo prebiehať formou večernej školy alebo diaľkového štúdia, aby bolo prístupné aj pracujúcim.

Pri pomaturitnom štúdiu kybernetickej bezpečnosti je nevyhnutné aby študenti spĺňali základné vedomosti a zručnosti v oblasti informačných technológií (napr. absolvovaný odbor 2563 M Informačné a sieťové technológie). Z tohto dôvodu by pomaturitné štúdium plne korešpondovalo s inováciou odboru 2561 M Informačné a sieťové technológie.

Ďalšou možnosťou pre pomaturitné štúdium pre oblasť kybernetickej bezpečnosti je špecializácia, alebo zameranie sa viac na manažment kybernetickej bezpečnosti. Tento typ štúdia by mohol efektívne prepájať teoretické vedomosti s praktickými zručnosťami a pripravovať absolventov na riadenie a koordináciu bezpečnostných opatrení v organizáciách. Študijný program by mohol zahŕňať najmä oblasti ako základy kybernetickej bezpečnosti, manažment rizík, bezpečnostné štandardy a normy, bezpečnostné politiky a postupy, bezpečnostné technológie, riešenie incidentov, bezpečnostné povedomie, právne a etické aspekty, manažérske zručnosti.

Predpoklady pre štúdium manažmentu kybernetickej bezpečnosti sú mierne odlišné od predpokladov pre špecialistov na kybernetickú bezpečnosť. Zatiaľ čo špecialisti potrebujú hlboké technické vedomosti a zručnosti, manažéri by mali mať skôr širší prehľad o problematike a schopnosť aplikovať manažérske princípy v oblasti kybernetickej bezpečnosti.

Pomaturitné štúdium zamerané na manažment kybernetickej bezpečnosti by mohlo byť efektívnym spôsobom, ako pripraviť kvalifikovaných odborníkov na riadenie a koordináciu bezpečnostných opatrení v organizáciách. Poskytlo by dodatočné informácie, ktoré sú relevantné pre riadenie aktivít a činností v oblasti kybernetickej bezpečnosti v organizáciách. Dôležité je však správne definovať obsah štúdia a predpoklady pre študentov, aby absolventi mali relevantné vedomosti a zručnosti pre prax.

Aj keď sú predpoklady štúdium manažmentu kybernetickej bezpečnosti mierne odlišné pre dosiahnutie dostatočnej kvalifikácie je vhodné disponovať silnejším technologickým základom. Štúdium manažmentu kybernetickej bezpečnosti ako nadstavba je vhodnejšie pre absolventov, ktorí už majú minimálne 2 – 3 roky praxe na pozícii špecialistu.

Vzhľadom na potrebu hlbších technologických vedomostí je vhodnejšie zamerať sa na dlhodobejšie formy vzdelávania, ktoré umožnia študentom získať komplexné vedomosti a zručnosti v oblasti kybernetickej bezpečnosti a zároveň sa prispôsobiť dynamickému vývoju v tejto oblasti.

Vyhodnotenie komparatívnej analýzy

Na základe porovnania štátnych vzdelávacích programov zo skupiny odborov 25 a 26, porovnaním rámcových učebných plánov a ich celkového zamerania je možné vysloviť záver, že pre oblasťou kybernetickej bezpečnosti je vhodnejšie pracovať v skupine odborov 25, ktoré poskytujú najširšiu a najadekvátnejšiu škálu potrebných vedomostí.

Pre vzdelávanie odborníkov v oblasti kybernetickej bezpečnosti je najvhodnejším prístupom inovácia odboru 2561 M Informačné a sieťové technológie. Inovácia by mala byť navrhnutá formou zamerania využitím voliteľných predmetov pre 3. a 4. ročník, tak aby mal absolvent by mal po absolvovaní 2. ročníka možnosť výberu zamerania. Jedným zo zameraní by tak bol - Špecialista kybernetickej bezpečnosti. Uvedený rozsah a obsah inovácie je uvedený nižšie v texte tohto dokumentu.

Špecialista kybernetickej bezpečnosti by sa špecializoval na kybernetickú bezpečnosť serverov, sietí, koncových bodov, webových aplikácií, kryptografiu, programovanie, právnu výchovu a manažment bezpečnostných rizík.

Študijný odbor 2561 M Informačné a sieťové technológie poskytuje študentom potrebný technologický základ, ktorý sa dá vhodne doplniť odbornými predmetmi zameranými na kybernetickú bezpečnosť. Tento prístup je najvhodnejší aj z pohľadu rýchlosti jeho zavedenia ako aj z pohľadu dostatočnej flexibility aplikácie nových poznatkov a trendov do výučby.

NÁVRH INOVATÍVNEHO ŠTÁTNEHO VZDELÁVACIEHO PROGRAMU

Popis vzdelávacieho programu

Odborné vzdelávanie a príprava v inovovanom študijnom obore 2561 M Informačné a sieťové technológie zahŕňa teoretické vyučovanie a praktickú prípravu žiakov, ktorí úspešne ukončili 9. ročník základnej školy.

Cieľom odborného vzdelávania a prípravy v tomto študijnom odbore je reagovať na naliehavé potreby trhu a zvýšiť počet kvalifikovaných stredných technických odborníkov pre oblasť kybernetickej bezpečnosti. Štvorročný odbor štúdia je koncipovaný homogénne ako odbor profesijnej prípravy pre zabezpečovanie ochrany informačných systémov v organizáciách, ktoré spočíva v zisťovaní a hodnotení možných bezpečnostných hrozieb, návrhu, nasadzovaní a prevádzke primeraných bezpečnostných opatrení na ich ošetrenie ako aj monitorovanie ich efektívnosti a kontinuálne zlepšovanie celkovej úrovne kybernetickej bezpečnosti.

Stratégia výučby vytvára priestor na rozvoj nielen odborných, ale aj všeobecných a kľúčových kompetencií. Najväčší dôraz sa kladie na komplexný rozvoj osobnosti žiaka. Všeobecná zložka vzdelávania vychádza zo skladby všeobecnovzdelávacích predmetov učebného plánu. V jazykovej oblasti je vzdelávanie a príprava zameraná na slovnú a písomnú komunikáciu v slovenskom jazyku, na vyjadrovanie sa v bežných situáciách spoločenského a pracovného styku, ale aj porozumenie technickej dokumentácie v cudzom jazyku. Žiak sa tiež oboznamuje s vývojom ľudskej spoločnosti, základnými princípmi etiky, zásadami spoločenského správania, osvojuje si základy matematiky, fyziky a informatiky, ktoré sú nevyhnutné pre výkon povolania.

Teoretická príprava v odbornom vzdelávaní je zameraná na poznatky z oblasti informačných a komunikačných technológií a kybernetickej bezpečnosti a ich vzájomnej prepojenosti. Rovnako poskytne aj ucelený obraz o holistickom prístupe k riadeniu kybernetickej bezpečnosti v organizáciách v súlade s jej poslaním, strategickými cieľmi ako aj platnou legislatívou.

Dôležitou súčasťou odborného vzdelávania je praktická príprava, ktorá umožňuje absolventovi získať potrebné praktické zručnosti pre pozíciu špecialista kybernetickej bezpečnosti a to návrh architektúry, implementáciou, inštaláciu informačných systémov a bezpečnostných nástrojov, ich prevádzku a údržbu, vrátane zapojenia vyhradených technických zariadení v zmysle platnej legislatívy. Taktiež je kladený veľký dôraz aj na rozvoj osobnosti žiaka, na formovanie jeho osobnostných a profesionálnych vlastností, postojov a hodnotovej orientácie.

Prepojenie všeobecného a odborného vzdelávania umožňuje pripraviť osobnosť všestranne rozvinutú, adaptabilnú, schopnú uplatniť sa na súčasnom trhu práce. Absolvent vie pracovať samostatne aj viesť menšie tímy, logicky myslieť, uplatňovať zásady bezpečnosti pri práci, hygieny práce, ochrany pred požiarmi a ochrany životného prostredia v odbore. Má predpoklady konať cieľavedome, rozhodne a rozvážne v súlade s právnymi predpismi spoločnosti, zásadami vlastenectva, humanizmu a Demokracie. Predpokladá sa jeho schopnosť samostatného ďalšieho rozvoja, napr. formou vysokoškolského štúdia, ale najmä celoživotného vzdelávania v rámci odboru.

Základné údaje (možnosti pracovného uplatnenia absolventa)

Uplatnenie absolventov tohto študijného odboru bude v oblasti kybernetickej bezpečnosti a to v nepretržitom zaisťovaní ochrany informačných systémov pred narušením dostupnosti, dôvernosti a integrity spracúvaných údajov.

Získaním základných odborných vedomostí a zručností sa absolvent uplatní ako schopný samostatne vykonávať činnosti spočívajúce v zisťovaní a hodnotení možných bezpečnostných hrozieb, vytvorení bezpečnostnej architektúry, dizajne, implementácii a prevádzke bezpečnostných nástrojov, monitorovaní a testovaní ich efektivity, riešení incidentov ako aj spolupráci s externými partnermi. Na kvalifikované vykonávanie uvedených činností získava absolvent štúdiom široký odborný profil s nevyhnutným všeobecným vzdelaním, s dostatočnou adaptabilitou, logickým myslením a schopnosťou aplikovať nadobudnuté vedomosti pri riešení problémov samostatne aj v tíme.

Špecialista kybernetickej bezpečnosti má v organizácii širokú škálu zodpovedností, ktoré sú kľúčové pre ochranu jej informačných aktív a zabezpečenie plynulého chodu. Za týmto účelom vykonáva nasledovné úlohy:

- sledovanie aktuálnych kybernetických hrozieb, identifikácia potenciálnych hrozieb a zraniteľností v systémoch a sieťach organizácie, ako aj vyhodnotenie ich dopadu na chod organizácie, analýza rizík, testovanie zraniteľností,
- výber, inštalácia a konfigurácia bezpečnostných technológií a nástrojov (napr. firewally, antivírusové programy, systémy na detekciu vniknutia (IDS/IPS), systémy na prevenciu úniku dát (DLP) a pod.), zabezpečenie ich správneho fungovania, aktualizácie a monitorovania,
- zabezpečenie bezpečnej konfigurácie sietí, nastavenia prístupov a segmentácie siete,
- vypracovanie bezpečnostných politík a štandardov, zabezpečenie ich dodržiavania, zvyšovanie povedomia o kybernetickej bezpečnosti,
- Identifikácia a analýza kybernetických útokov a narušení bezpečnosti, implementácia opatrení na zmiernenie dopadov útokov a obnova systémov,
- zabezpečenie koordinácie a spolupráce s inými oddeleniami, informovanie manažmentu o bezpečnostných rizikách a navrhovanie opatrení na ich zmiernenie,
- implementácia a udržiavanie systému riadenia kybernetickej bezpečnosti podľa platnej legislatívy, alebo medzinárodných štandardov,
- monitorovanie a hodnotenie efektivity systému riadenia kybernetickej bezpečnosti a navrhovanie opatrení na jeho zlepšenie.

Zdravotné požiadavky na uchádzača

Odporúča sa lekárske posúdenie zdravotného stavu uchádzača o prijatie na tento študijný odbor. Odbor nie je vhodný pre žiaka so zmenenou pracovnou schopnosťou, najmä s mentálnym postihnutím ako mentálna retardácia, autizmus, poruchy správania, psychiatrické diagnózy a s vážnymi poruchami zraku a sluchu. V prípade zmenenej pracovnej schopnosti uchádzačov je potrebné potvrdenie o lekárskom posúdení zdravotnej spôsobilosti priložené k prihláške na štúdium.

PROFIL ABSOLVENTA

Celková charakteristika absolvent študijného odboru so zameraním Špecialista kybernetickej bezpečnosti

V digitálnom veku, kde sa informačné technológie stávajú neoddeliteľnou súčasťou našich životov, rastie aj potreba ich ochrany. Absolvent po úspešnom ukončení štúdia získava prvú kvalifikáciu na úrovni úplného stredného odborného vzdelania (maturitné vysvedčenie a výučný list). Zároveň absolvent získa vedomosti a zručnosti na výkon odborných činností v oblastiach kybernetickej bezpečnosti najmä v sieťovej bezpečnosti, bezpečnosti operačných systémov, programovania a skriptovania, databáz, kryptografie, bezpečnostného testovania, bezpečnostných nástrojov a technológií a tiež znalosti bezpečnostných štandardov a legislatívy.

Na kvalifikované vykonávanie odborných činností musí mať absolvent široký odborný profil s nevyhnutným všeobecným vzdelaním a zároveň by mal spĺňať požiadavky relevantnej legislatívy na prácu s vyhradenými zariadeniami. Musí byť dostatočne adaptabilný aj v príbuzných odboroch, logicky mysliaci, schopný aplikovať nadobudnuté vedomosti a schopnosti pri riešení problémov. Musí byť schopný pracovať samostatne i v kolektíve, sústavne sa vzdelávať a trvale sa zaujímať o vývoj a nové poznatky svojho odboru.

Absolvent ovláda zásady zaisťovania kybernetickej bezpečnosti, má osvojené základné princípy fungovania trhového mechanizmu, pozná metódy práce podnikateľa. Vie využívať informácie a právne normy súvisiace s rozvojom podnikania pri rôznych formách vlastníctva. Koná cieľavedome, rozvážne a rozhodne v súlade s právnymi normami a zásadami demokracie.

Absolvent inovovaného odboru je kvalifikovaný odborník s adekvátnymi znalosťami a zručnosťami v oblasti ochrany informačných systémov a sietí pred kybernetickými hrozbami. Je schopný analyzovať, navrhovať a implementovať bezpečnostné opatrenia na ochranu dát a infraštruktúry organizácií. Špecialista kybernetickej bezpečnosti sa zameriava na konkrétnu oblasť kybernetickej bezpečnosti, napríklad na sieťovú bezpečnosť, bezpečnosť operačných systémov, detekciu bezpečnostných incidentov, kryptovanie, alebo penetračné testovanie a pod. Ovláda relevantné nástroje a technológie a dokáže ich efektívne aplikovať pri identifikácii a analýze kybernetických hrozieb. Precíznosť, detailná orientácia a schopnosť riešiť problémy sú kľúčové pre jeho úspech. Dôležitá je aj schopnosť efektívne spolupracovať v tíme a záujem o celoživotné vzdelávanie, aby držal krok s neustále sa vyvíjajúcimi technológiami a hrozbami.

Špecialista musí ovládať cudzí jazyk, najmä angličtinu, a mať zručnosti v oblasti práce s počítačom a internetom. Musia byť schopní analyzovať problémové situácie, riešiť problémy a pracovať v skupine.

Absolvent má široké uplatnenie v rôznych sektoroch. Môžu pracovať v IT firmách, bankovníctve, verejnej správe, telekomunikáciách, energetike, zdravotníctve a priemysle. Po absolvovaní štúdia môžu pokračovať na vysokej škole alebo si zvyšovať kvalifikáciu rôznymi kurzami a certifikáciami.

Vzhľadom na rastúcu dôležitosť kybernetickej bezpečnosti a nedostatok kvalifikovaných odborníkov je absolvent tohto odboru cenným prínosom pre každú organizáciu.

Kľúčové kompetencie

Vzdelávanie podľa štátneho vzdelávacieho programu (ďalej len „ŠVP“) v súlade s cieľmi výchovy a vzdelávania na danom stupni vzdelania smeruje k tomu, aby si žiaci vytvorili zodpovedajúce schopnosti a študijné predpoklady. Kľúčové kompetencie chápeme ako kombináciu vedomostí, zručností, postojov, hodnotovej orientácie a ďalších charakteristík osobnosti, ktoré každý človek potrebuje na svoje osobné uspokojenie a rozvoj, aktívne občianstvo, spoločenské a sociálne začlenenie, k tomu, aby mohol primerane konať v rôznych pracovných a životných situáciách počas celého svojho života. Kľúčové kompetencie, konkretizované vo výkonových štandardoch, sa v rámci

výchovnovzdelávacieho procesu prostredníctvom výchovných a vzdelávacích stratégií rozvíjajú, osvojujú a hodnotia buď na úrovni školy, odboru vzdelávania alebo vyučovacieho predmetu. V súlade so Spoločným európskym rámcom kľúčových kompetencií pre celoživotné vzdelávanie ŠVP vymedzil nasledovné kľúčové kompetencie:

Spôsobilosti konať samostatne v spoločenskom a pracovnom živote

Sú to spôsobilosti, ktoré sú základom pre ďalšie získavanie vedomostí, zručností, postojov a hodnotovej orientácie. Patria sem schopnosti nevyhnutné na cieľavedomé a zodpovedné riadenie a organizovanie svojho osobného, spoločenského a pracovného života. Jednotlivci si potrebujú vytvárať svoju osobnú identitu vo vzťahu k životným podmienkam, povolaniu, práci a životnému prostrediu, spoločenským normám, sociálnym a ekonomickým inštitúciám, robiť správne rozhodnutia, voľby, opatrenia a postupy. Tieto kompetencie sú veľmi úzko späté s osvojovaním si kultúry myslenia a poznávania.

Absolvent má:

- logicky a reálne zdôvodňovať svoje názory, konania a rozhodnutia,
- porovnať formálne a neformálne pravidlá, zákonitosti, predpisy, sociálne normy,
- morálne zásady, vlastné a celospoločenské očakávania v systéme, v ktorom existuje,
- identifikovať priame a nepriame dôsledky svojej činnosti,
- vybrať si a vhodne zdôvodniť správne rozhodnutie a cieľ z rôznych možností,
- vysvetliť svoje pracovné, prípadne životné plány, záujmy a predsavzatia,
- popísať svoje ľudské práva, popísať svoje povinnosti, záujmy, obmedzenia a potreby,
- definovať svoje ciele a prognózy najmä v kontexte pracovných činností,
- určiť zdroje osobného a spoločenského života a ich očakávaný vývoj, zdôvodňovať svoje argumenty, riešenia, potreby, práva, povinnosti a konanie.

Spôsobilosti interaktívne používať vedomosti, informačné a komunikačné technológie, komunikovať v štátnom, materinskom a cudzom jazyku

Sú to schopnosti, ktoré žiak získava na aktívne zapojenie sa do spoločnosti založenej na vedomostiach s jasným zmyslom pre vlastnú identitu a smer života, sebazdokonaľovanie a zvyšovanie výkonnosti, racionálne a samostatné vzdelávanie a učenie sa počas celého života, aktualizovanie a udržovanie potrebnej základnej úrovne jazykových schopností, informačných a komunikačných zručností. Od žiaka sa vyžaduje efektívne využívať písaný a hovorený materinský a cudzí jazyk, disponovať čitateľskou, matematickou a digitálnou gramotnosťou, prehodnocovať základné zručnosti.

Absolvent má:

- správne sa vyjadrovať v materinskom jazyku v písomnej a hovorenej forme,
- spoľahlivo sa vyjadrovať v cudzom jazyku v písomnej a hovorenej forme,
- riešiť problémové situácie s využitím matematického aparátu,
- identifikovať, vyhľadať, analyzovať, usporiadať, overovať, interpretovať a uložiť dáta, informácie a digitálny obsah pre riešenie úloh a zadaní,
- zvoliť a použiť digitálne technológie a nástroje na komunikáciu, vrátane elektronickej pošty, zdôvodniť zásady netikety.
- vytvoriť a editovať digitálny obsah, integrovať jeho časti, použiť príkazy pre výpočtový systém,

- uplatniť a vysvetliť spôsoby na ochranu informačnej bezpečnosti používaných zariadení a ochrany digitálneho obsahu,
- rozlíšiť technické problémy IKT, vybrať spôsoby ich riešenia, zdôvodniť vlastné informačné potreby
- posudzovať vierohodnosť rôznych informačných zdrojov,
- kriticky hodnotiť získané informácie,
- formulovať jednoduché hypotézy, pozorovať, triediť a merať.

Schopnosť pracovať v rôznorodých skupinách

Tieto schopnosti sa využívajú pri riadení medziľudských vzťahov, formovaní nových typov spolupráce. Sú to schopnosti, ktoré sa objavujú v náročnejších podmienkach, aj pri riešení problémov ľudí, ktorí sa nevedia zaradiť do spoločenského života. Žiaci musia byť schopní učiť sa, nažívať a pracovať nielen ako jednotlivci, ale v sociálne vyváženej skupine. Sú to teda schopnosti, ktoré na základe získaných vedomostí, sociálnych zručnosti, interkulturálnych kompetencií, postojov a hodnotovej orientácie umožňujú stanoviť jednoduché algoritmy na vyriešenie problémových úloh, javov a situácií a získané poznatky využívať v osobnom živote a povolaní.

Absolvent má:

- prejaviť empatiu a sebareflexiu,
- vyjadriť svoje pocity a korigovať negativitu,
- pozitívne motivovať seba a druhých,
- používať argumenty na ovplyvňovanie ľudí (prehováranie, presvedčovanie),
- stanoviť priority cieľov,
- predkladať primerané návrhy na rozdelenie jednotlivých kompetencií a úloh pre ostatných členov tímu a posudzovať spoločne s učiteľom a s ostatnými, či sú schopní určené kompetencie zvládnuť,
- Vhodnou formou prezentovať svoje myšlienky, návrhy a postoje,
- konštruktívne diskutovať, aktívne predkladať progresívne návrhy a pozorne počúvať druhých,
- prispieť k riešeniu konfliktných situácií v meniacich sa podmienkach, pri rešpektovaní etických noriem a akceptovaní rozdielnych názorov,
- budovať a organizovať vyrovnanú a udržateľnú spoluprácu,
- uzatvárať jasné dohody a dodržiavať ich,
- spolurozhodnúť o výbere správneho názoru z rôznych možností,
- analyzovať hranice zvereného problému alebo situácie,
- identifikovať oblasť dohody a rozporu,
- určovať najzávažnejšie rysy problému, rôzne možnosti riešenia, ich klady a zápory v danom kontexte aj v dlhodobejších súvislostiach, kritériá pre voľbu konečného optimálneho riešenia,
- spolupracovať pri riešení problémov s inými ľuďmi,
- samostatne pracovať a riadiť práce v menšom kolektíve,
- určovať vážne nedostatky a kvality vo vlastnom učení, pracovných výkonoch a osobnostnom raste,
- predkladať spolupracovníkom vlastné návrhy na zlepšenie práce, bez zaujatosti posudzovať návrhy druhých,
- prispievať k vytváraniu ústretových medziľudských vzťahov, predchádzať osobným konfliktom, nepodliehať predsudkom a stereotypom v prístupe k druhým.

ODBORNÉ KOMPETENCIE

Požadované vedomosti

Absolvent má:

- popísať a vysvetliť základné princípy pre konštrukciu, štruktúru a činnosť hardvéru počítača, jeho jednotlivých častí a celku a s tým súvisiacich pojmov (CPU, RAM, HDD, I/O port a pod.),
- vysvetliť základnú terminológiu pre prácu s IKT systémami (byte, MB, ,exe, skript, firmware, IP adresa a pod.),
- používať základné pracovné postupy pri inštalácii, údržbe a montáži technických prostriedkov IKT systémov,
- popísať a vysvetliť základné koncepty vytvárania sietí a ich bezpečnosti (dráha/route, sieť, nslookup a pod.) a sieťových komponentov (prepínač, smerovač, firewall, LAN, WAN, port a pod.),
- charakterizovať a vysvetliť účel komunikačných protokolov používaných pre IKT systémy (najmä TCP/IP, UDP a pod.),
- ovládať terminológiu a základné pracovné postupy pre návrh integrovaných IKT riešení, prácu s nimi, odbornú správu a odstraňovanie porúch v komplexnejších a integrovaných IKT riešeniach a aplikáciách,
- popísať formy a možnosti krátkodobého, resp, dlhodobého uloženia údajov v IKT systémoch a charakterizovať dátové úložiská prístupné cez sieť, so zvýšenou úrovňou zabezpečenia dát proti stratám a pod.,
- charakterizovať a vysvetliť účel, princíp a postupy pre využitie značkovacích jazykov (HTML, XML a pod.) v tvorbe webových stránok a riešení,
- poznať základnú odbornú terminológiu a symboliku súvisiacu s informačnou a kybernetickou bezpečnosťou,
- orientovať sa v zákonoch, ktoré sa zaoberajú prvkami informačnej bezpečnosti,
- poznať princípy, obsah a vhodné spôsoby práce s normami, katalógmi, firemnými manuálmi a projektovou dokumentáciou,
- orientovať sa v systéme noriem ISO 27000,
- vedieť vysvetliť, prečo je digitalizácia života prirodzeným krokom vývoja a vedieť použiť príklad,
- prirodzene používať pojem digitálny priestor, digitálna identita,
- popísať a vysvetliť praktiky sociálneho inžinierstva, manipulatívne techniky a príklady jednotlivých typov útokov na používateľov, pomocou techník sociálneho inžinierstva,
- vysvetliť rozdiel medzi digitálnou stopu a auditným záznamom a logom a identifikovať, kde sa ktorý záznam v systémoch IKT nachádza,
- poznať princípy informačnej bezpečnosti: CIA, need to know, need to do a implementovať na jednotlivé prvky informačnej bezpečnosti (IKT, ľudia, procesy),
- vedieť popísať čo sú osobné údaje a prčo ich musíme chrániť a implementovať požiadavky na ochranu osobných údajov v emaile, čete a na sociálnych sieťach,
- popísať a vysvetliť základné techniky programovania aspoň v jednom vyššom programovacom a/alebo skriptovacom jazyku (Java, C++, Python, PHP a pod.),
- ovládať terminológiu a základné pracovné postupy pre zabezpečenie systémov IKT na úrovni prvkov infraštruktúry, dát, procesov, vrátane ich dostupnosti a kontinuity,
- určiť rámcové bezpečnostné hrozby a zraniteľnosti na úrovni operačného systému a štandardného aplikačného programového vybavenia serverov a pracovných staníc,
- určiť rámcové bezpečnostné hrozby a zraniteľnosti databáz (databázové systémy),
- používať prirodzene v kontexte slovo riziko, aktívum zraniteľnosť a vedieť ich implementovať na bežné veci, okolo seba,

- každú aktivitu v informačnej bezpečnosti vnímať ako proces so svojimi aktivitami, pravidlami a životným cyklom,
- navrhovať, spoločným rozhodnutím pretvárať existujúce procesy informačnej bezpečnosti,
- ovládať terminológiu a základné pracovné postupy procesného a projektového riadenia moderných IKT riešení,
- popísať základné pojmy týkajúce sa ekonomiky podniku, trhového mechanizmu, riadenia podniku a firmy, mzdovej a pracovno-právnej problematiky, oceňovania a predaja výrobkov a služieb,
- definovať a charakterizovať terminológiu IKT služieb a ich rolu v riadení moderných IKT riešení,
- vysvetliť rozdiel medzi počítačom, smartfónom a IoT zariadením,
- popísať prvky kybernetického útoku a jeho jednotlivých prvkov: vektor útoku, rozsah, dopad, cieľ,
- Vymenovať a vysvetliť princípy vybraných kybernetických útokov zameraných na počítač v ponímaní jednotlivých prvkov a so zameraním na možnosť ochrany pomocou antivírusu,
- Popísať princíp fungovania internetového prehliadača, jeho jednotlivých prvkov, Vedieť vysvetliť útoky na domény a ochranu pred takto zameranými útokmi,
- vedieť popísať funkcionalitu emailu a garanciu správy a možnosti nastavenia a ochrany (MFA, výber poskytovateľa elektronickej pošty,
- schopnosť práce s emailom, vytváranie filtrov, analýza tela emailu, kontrola používaného smtp servera, zapnutie SMTPS a overenie SPF záznamu,
- vedieť vysvetliť rozdiel medzi správami typu SPAM, HOAX a dezinformácia,
- definovať pojem projektu v kontexte IKT a charakterizovať typické fázy projektu a aktivity s nimi súvisiace,
- vnímať heslo ako tajný bezpečnostný reťazec, vedieť vysvetliť spôsob generovania hesla, popísať požiadavky na generovanie bezpečného hesla, vedieť vysvetliť vybrané útoky na heslo,
- vysvetliť princípy multifaktorovej autentizácie,
- vysvetliť jednotlivé ciele, na ktoré sa útočníci zameriavajú (priame a nepriame ciele) a spôsoby infiltrácií a vysvetlenie, prečo sa nesmie používať jailbreak a rootkit na mobilných zariadeniach,
- poznať zásady práce s príslušným softvérovým vybavením počítača a mobilného zariadenia pri riadení bezpečnosti a jeho súčastí,
- popísať a vysvetliť základné koncepty vytvárania jednoduchých komunikačných sietí a ich bezpečnosti (počítačová sieť, cesta v sieti, preklad adresy a pod.) a sieťových komponentov (prepínač, smerovač, firewall, LAN, WAN, port a pod.),
- poznať zásady práce s príslušným softvérovým vybavením sieťových komponentov (touter, firewall, Next Generation Firewall, IPS,,,,) pri riadení bezpečnosti a jeho súčastí,
- charakterizovať základné kontrolné programy a metódy na overenie bezpečnosti a vytvorenie ochranných krokov,
- orientovať sa v základných druhoch materiálov a polotovarov používaných v pri správe sietí ich druhy, vlastnosti a použitie,
- popísať základné súčiastky, prvky, rozvody a obvody používané v pri správe sietí,
- charakterizovať a vysvetliť účel komunikačných protokolov používaných pre komunikáciu medzi lokálnymi a vzdialenými IKT systémami (najmä Ethernet, IP, TCP, UDP a pod.),
- charakterizovať ekonomické aspekty v podnikaní v kontexte a odboroch IKT, podnikateľské modely firiem, princípy riadenia a organizačné formy firiem, základné finančné koncepty, marketingové a obchodné postupy, riziká a ich aktívne riadenie, zásady trhového mechanizmu,
- ovládať terminológiu a základné pracovné postupy pre efektívnu spoluprácu s odberateľmi a používateľmi IKT systémov a riešení,

- ovládať terminológiu a základné pracovné postupy pre efektívnu komunikáciu so zákazníkom, používateľom a tímom,
- ovládať terminológiu a základné pracovné postupy pre prácu s informáciami, ich získavanie, spracovanie a analýzu,
- charakterizovať pojem a úlohu informácie, informovania a informatických služieb v modernej spoločnosti od komunikácií až po multimediálne dokumenty,
- popísať a vysvetliť potrebu dokumentácie v moderných IKT systémoch a riešeniach, najmä pri návrhu a vývoji softvérových riešení,
- popísať dostupné systémy pre hľadanie, získavanie a prácu s informáciami, vrátane didaktických aplikácií pre podporu odborného vzdelávania v IKT,
- vysvetliť zásady bezpečnosti a ochrany zdravia pri práci, ochrany pred požiarom,
- vysvetliť zásady ochrany životného prostredia pri vykonávaní stavebnej činnosti, spôsob nakladania so vzniknutým odpadom a jeho vplyv na životné prostredie,
- vysvetliť zásady bezpečnosti a ochrany zdravia pri práci s technickými,
- ovládať terminológiu bezpečnostných štandardov a vysvetliť dôvod existencie,
- popísať dôvod existencie vzdelávania informačnej bezpečnosti v praxi
- vysvetliť prepojenie informačnej bezpečnosti s cieľmi organizácie cez stratégiu organizácie,
- popísať jednotlivé prvky, z čoho sa stratégia organizácie skladá (pojem: misia, vízia, hodnoty, SWOT, ukazovatele stratégie, ciele, úlohy),
- vysvetliť, prečo organizácia potrebuje bezpečnostné politiky a aké sú odporúčania na ošetrenie výnimiek,
- vymenovať jednotlivé prvky riadenia informačnej bezpečnosti organizácie a právne ich zaradiť do úrovní riadenia a vymenovať typické zodpovednosti,
- vymenovať jednotlivé prvky zodpovednosti za nastavenie informačnej bezpečnosti (biznis vlastní, informačný vlastník, používateľ,
- vedieť vysvetliť, na čo slúži Dohoda o poskytovaní služieb (SLA),
- vysvetliť, prečo je dôležitý bezpečnostný princíp oddelenie pávomocí (segregation of duties),
- vymenovať jednotlivé prvky a zodpovednosti v projektovom riadení do zahrnutím informačnej bezpečnosti,
- popísať potrebu ochrany mobilných zariadení
- ovládať požiadavky kladené na prácu z domu a v rozumnom miere ich vedieť nastaviť, vyžadovať a kontrolovať,
- rozumieť cieľom a potrebám personálnej bezpečnosti od prípravy pred nastúpením do zamestnania, cez podmienky zamestnania, správnom nastavení pracovnej náplni, požiadavkám na politiku informačnej bezpečnosti až po ukončenie zamestnania,
- vysvetliť, čo je to aktívum a vlastníctvo aktív a vedieť popísať životný cyklus od zavedenia až po spôsob vrátenia aktív,
- nastaviť označovanie citlivosti dokumentov a všetkých druhov aktív, Vedieť aplikovať požiadavky na citlivosť informácií aj na jednotlivé typy médií,
- vedieť vysvetliť rozdiel medzi autentifikáciou a autorizáciou a popísať požiadavky na politiku prístupových práv a princípy na riadenie prístupových práv,
- nastaviť základné pravidlá pre sieťovú bezpečnosť,
- ovládať tému kryptografie a vedieť implementovať re vybrané systémy kryptografické opatrenia, v miere: symetrická šifra, asymetrická šifra, digitálny podpis a hash,

- poznať základnú odbornú terminológiu a symboliku a pravidlá súvisiace s fyzickou bezpečnosťou,
- vysvetliť potreby implementovania politiky čistého stola a potreby vyžadovania dodržiavania v organizácií,
- ovládať tému bezpečnosti prevádzky manažment prevádzky, zdokumentovanie procesov na základe metodiky ITIL, riadenie zmien a kapacít, oddelenie prostredí,
- poznanie práva duševného vlastnéctva a implementáciu práva na dennú prácu v informačnej bezpečnosti,
- vysvetliť potrebu existencie nezávislého auditu a overovania technického súladu s existujúcim nastavením.

Požadované zručnosti

Absolvent vie:

- používať na úrovni bežného používateľa bežné OS (Windows, Linux a pod.) pre všeobecné účely (kopírovanie, archivovanie, nastavovanie, editovanie a pod.),
- diagnostikovať prevádzkyschopnosť a funkčnosť počítačových sietí,
- riešiť jednoduché problémy integrácie IKT z praxe a zvoliť s ohľadom na technické a ekonomické požiadavky správne postupy riešenia,
- plynule používať internet a sieťové služby (email, vyhľadávač, web, vzdialený prístup, ssh, scp a pod.),
- získavať a interpretovať požiadavky zákazníka na softvérovú aplikáciu,
- sledovať základné údaje a vykonávať postupy týkajúce sa počítačovej bezpečnosti (antivírus, heslá, prístupy a pod.),
- definovať bezpečnostnej politiky IS a jej implementácia,
- kontrolovať dodržiavanie bezpečnostných pravidiel, postupov a procedúr,
- aplikovať základné koncepty projektového manažmentu na jednoduché projektové činnosti (definícia rozsahu, plánu, stavu a pod.),
- vykonávať základné pracovné postupy pri efektívnej spolupráci s odberateľmi a používateľmi IKT systémov a riešení,
- pochopiť situáciu z pohľadu zákazníka a spresniť potreby a želania zákazníka podľa potreby,
- prezentovať pred menším publikom,
- dodržiavať etické normy, správať sa transparentne voči druhým a rešpektovať ich hodnoty a individualitu,
- podnecovať spoluprácu a prácu v tíme a prispievať k produktívnej atmosfére v tíme,
- komunikovať ústne a písomne vhodným spôsobom vzhľadom na cieľové publikum a situáciu,
- vykonávať základné pracovné postupy pri práci s informáciami, ich získavaní, spracovaní a analýze,
- využívať aplikačné a špecifické softvéry systémov informačných, serverových a sieťových technológií a databáz,
- používať vyhľadávače a iné zdieľané zdroje (wiki, QBase a pod.) za účelom efektívneho získania informácií pre riešenie úloh a problémov IKT,
- využívať aplikačné programy na spracovanie textu, tabuľkové procesory, nástroje na tvorbu prezentácií, databáz, grafiky a technickej dokumentácie v oblasti IKT a príbuzných odboroch,
- zbierať údaje, abstrahovať a sumarizovať informácie z viacerých zdrojov využívajúc vhodné kancelárske balíky a aplikácie,
- efektívne vytvárať a predkladať správy o stave pridelených úloh a činností s využitím nástrojov tabuľkových procesorov, prezentácií a dokumentov,

- navrhovať, zostavovať a prepracovávať odborné dokumenty a dokumentáciu (správy, prehľady, návrhy, zdôvodnenia, zápisnice, emaily a pod.),
- vytvárať dokumentáciu opisujúcu produkt, službu, IKT komponent, softvér, aplikáciu či webové riešenie,
- vysvetliť zásady bezpečnosti a ochrany zdravia pri práci, ochrany pred požiarom,
- vysvetliť zásady ochrany životného prostredia pri vykonávaní stavebnej činnosti, spôsob nakladania so vzniknutým odpadom a jeho vplyv na životné prostredie,
- vysvetliť zásady bezpečnosti a ochrany zdravia pri práci s technickými,
- ovládať terminológiu bezpečnostných štandardov a vysvetliť dôvod existencie,
- popísať dôvod existencie vzdelávania informačnej bezpečnosti v praxi
- vysvetliť prepojenie informačnej bezpečnosti s cieľmi organizácie cez stratégiu organizácie,
- popísať jednotlivé prvky, z čoho sa stratégia organizácie skladá (pojem: misia, vízia, hodnoty, SWOT, ukazovatele stratégie, ciele, úlohy),
- vysvetliť, prečo organizácia potrebuje bezpečnostné politiky a aké sú odporúčania na ošetrenie výnimiek,
- vymenovať jednotlivé prvky riadenia informačnej bezpečnosti organizácie a právne ich zaradiť do úrovní riadenia a vymenovať typické zodpovednosti,
- vymenovať jednotlivé prvky zodpovednosti za nastavenie informačnej bezpečnosti (biznis vlastní, informačný vlastník, používateľ,
- vedieť vysvetliť, na čo slúži Dohoda o poskytovaní služieb (SLA),
- vysvetliť, prečo je dôležitý bezpečnostný princíp oddelenie pávomocí (segregation of duties),
- vymenovať jednotlivé prvky a zodpovednosti v projektovom riadení do zahrnutím informačnej bezpečnosti,
- popísať potrebu ochrany a spôsob ochrany mobilných zariadení,
- ovládať požiadavky kladené na prácu z domu a v rozumnom miere ich vedieť nastaviť, vyžadovať a kontrolovať,
- rozumieť cieľom a potrebám personálnej bezpečnosti od prípravy pred nastúpením do zamestnania, cez podmienky zamestnania, správnom nastavení pracovnej náplni, požiadavkám na politiku informačnej bezpečnosti až po ukončenie zamestnania,
- vysvetliť, čo je to aktívum a vlastníctvo aktív a vedieť popísať životný cyklus od zavedenia až po spôsob vrátenia aktív,
- nastaviť označovanie citlivosti dokumentov a všetkých druhov aktív, Vedieť aplikovať požiadavky na citlivosť informácií aj na jednotlivé typy médií,
- vedieť vysvetliť rozdiel medzi autentifikáciou a autorizáciou a popísať požiadavky na politiku prístupových práv a princípy na riadenie prístupových práv,
- nastaviť základné pravidlá pre sieťovú bezpečnosť,
- ovládať tému kryptografie a vedieť implementovať re vybrané systémy kryptografické opatrenia, v miere: symetrická šifra, asymetrická šifra, digitálny podpis a hash,
- poznať základnú odbornú terminológiu a symboliku a pravidlá súvisiace s fyzickou bezpečnosťou,
- vysvetliť potreby implementovania politiky čistého stola a potreby vyžadovania dodržiavania v organizácií,
- vedieť posúdiť a vyhodnotiť jednotlivé udalosti informačnej bezpečnosti, vedieť štruktúrovane riadiť odstránenie incidentu informačnej bezpečnosti a poznať základy forenzného zberu dôkazov,
- poznať základy manažmentu kontinuity činností, vedieť vytvoriť plán kontinuity biznisu, vedieť otestovať plán kontinuity biznisu,

- ovládať tému bezpečnosti prevádzky manažment prevádzky, zdokumentovanie procesov na riadenie prevádzky, riadenie prevádzkového procesu, nastaviť oddelenie prostredí,
- nasadiť jednotlivé ochranné kroky voči malware,
- nastaviť ochranu servera a počítača a mobilného zariadenia na základe odporúčaní (napr. CisCatalog) a overiť funkčnosť ochrany.

Požadované osobnostné predpoklady, vlastnosti a schopnosti

Absolvent sa vyznačuje:

- dôslednosťou a zodpovednosťou pri riešení pracovných povinností,
- samostatnosťou pri práci, samostatným riešením bežných úloh,
- kreatívnym myslením,
- schopnosťou integrácie a adaptability
- organizačnými a komunikatívnymi vlastnosťami,
- prispôsobivosťou v nových pracovných podmienkach,
- vhodným sociálnym správaním a prejavmi,
- sebadisciplínou a mobilitou,
- potrebnou dávkou sebadôvery a pozitívnym prístupom k povinnostiam.

ŠKOLSKÝ VZDELÁVACÍ PROGRAM PRE ODBOR 2561 M INFORMAČNÉ A SIEŤOVÉ TECHNOLÓGIE ROZŠÍRENÝ O KYBERNETICKÚ BEZPEČNOSŤ

Vzdelávanie v oblasti kybernetickej bezpečnosti na stredných školách je nevyhnutné z dôvodu rastúcej digitálnej transformácie a čoraz zložitejších kybernetických hrozieb, ktorým čelí spoločnosť, podniky i jednotlivci. V súčasnosti, keď sa informačné technológie stali neoddeliteľnou súčasťou každodenného života, je ochrana digitálnych systémov a dát pred kybernetickými útokmi kľúčovým aspektom pre zabezpečenie nielen národnej bezpečnosti, ale aj ochrany osobných a firemných informácií.

Na stredných školách, kde žiaci nadobúdajú odborné znalosti a praktické zručnosti, je potrebné začleniť výučbu kybernetickej bezpečnosti do vzdelávacieho procesu. Tento krok umožní mladým ľuďom získať základné i pokročilé poznatky v oblasti ochrany digitálnych systémov, bezpečnosti sieťovej infraštruktúry, detekcie a prevencie kybernetických útokov, ako aj etických a právnych aspektov kybernetickej bezpečnosti.

V rámci analýzy vzdelávacích prístupov k problematike kybernetickej bezpečnosti sme preskúmali možnosti vytvorenia nového predmetu, ako aj alternatívu v podobe rozšírenia existujúcich predmetov o hlbšie a špecializovanejšie vzdelávanie v oblasti informačnej bezpečnosti. Na základe analýzy sme dospeli k odporúčaniu, aby sa väčší dôraz kládol na integráciu prvkov informačnej bezpečnosti do odborných predmetov. Vytvorili sme zoznam odborných kompetencií, ktoré zohľadňujú požiadavky štátneho vzdelávacieho programu, potreby školy a požiadavky trhu práce.

Na základe týchto zistení sme navrhli úpravy vybraných predmetov tak, aby pokryli potreby čo najväčšieho počtu stredných odborných škôl. Tieto predmety sú často súčasťou školských vzdelávacích programov.

Školský vzdelávací program, ktorý je podľa školského zákona základným pedagogickým dokumentom školy, sa vypracováva na základe Štátneho vzdelávacieho programu. Odráža ciele a zameranie školy, ako aj stratégiu určenú vedením školy v spolupráci s regiónom a obcou. Tento program zároveň zohľadňuje potreby a možnosti žiakov a pedagogického zboru. Pri jeho tvorbe škola využíva voliteľné hodiny a zostavuje vlastný učebný plán. V školskom učebnom pláne sú rozpracované všetky dostupné hodiny, ktoré škola môže využiť na výučbu.

Pre úspešnú implementáciu zmien je nevyhnutné, aby škola mala vypracovaný konkrétny učebný plán, ktorý zahrňuje aj nové predmety alebo úpravy existujúcich predmetov. V prípade škôl s rôznymi odbornými zameraniami môže byť vypracovaných viacero školských učebných plánov. V učebnom pláne sú zahrnuté aj nové predmety, ktoré škola zvolila, a sú podrobne uvedené aj metódy realizácie prierezových tém. Každá škola, ktorá zvýši počet hodín pre konkrétny predmet podľa štátneho vzdelávacieho programu, musí vypracovať aj podrobné učebné osnovy.

Výsledkom našej analýzy sú konkrétne úpravy obsahu vybraných tematických oblastí, ako sú predmety Operačné systémy, Prax a rozšírenie predmetu Operačné systémy Linux a Windows, často označovaného ako Serverové technológie. Okrem toho sme pripravili aj úpravy predmetu Kybernetická bezpečnosť. Na nasledujúcich stránkach predstavíme podrobnosti o týchto zmenách, ktoré sa zameriavajú na rozšírenie odborných poznatkov v oblasti informačnej a kybernetickej bezpečnosti. Praktický obsah predmetov zostáva nezmenený, pričom úpravy sa týkajú predovšetkým tých častí, ktoré sú odborné a priamo viazané na bezpečnostné aspekty, ako aj návrhov na úpravu vyučovacích hodín. Samotná implementácia týchto zmien je v kompetencii každej jednotlivé školy.

Pre príklad uvádzame učebný plán pre študijný odbor SPŠ Jozefa Murgaša Banská Bystrica:

Učebný plán pre študijný odbor 2561 M Informačné a sieťové technológie

Šk. rok: 2025/2026

Triedy: I. A, I. B, II. A, II. B, III. A, III. B, IV. A, IV. B

Škola	SPŠ Jozefa Murgaša, Hurbanova 6, 975 18 Banská Bystrica
Názov ŠkVP	INFORMAČNÉ A SIEŤOVÉ TECHNOLÓGIE
Kód a názov ŠVP	25 Informačné a komunikačné technológie
Kód a názov študijného odboru	2561 M Informačné a sieťové technológie
Stupeň vzdelania	ISCED 3A – úplné stredné odborné vzdelanie
Dĺžka štúdia	4 roky
Forma štúdia	denná
Vyučovací jazyk	slovenský jazyk

Kategórie a názvy vyučovacích predmetov	**Počet týždenných vyučovacích hodín v ročníku**				
	1.	**2.**	**3.**	**4.**	**spolu**
VŠEOBECNÉ VZDELÁVANIE	**19**	**19**	**14**	**15**	**67**
Jazyk a komunikácia	6	6	6	6	24
Slovenský jazyk a literatúra	3	3	3	3	12
Prvý cudzí jazyk (anglický jazyk)	3/3	3/3	3/3	3/3	12
Človek a hodnoty	1	1	0	0	2
Etická výchova/náboženská výchova a)	1	1	-	-	2
Človek a spoločnosť	2	2	1	0	5
Dejepis	1	1	-	-	2
Občianska náuka	1	1	1	-	3
Človek a príroda	2	1	0	0	3
Fyzika	2	1	-	-	3
Matematika a práca s informáciami	2	2	2	0	6
Matematika b)	2	2	2	-	6
Zdravie a pohyb	2	2	2	2	8

Telesná a športová výchova	2	2	2	2	8
Disponibilné hodiny	4	5	3	7	19
Druhý cudzí jazyk c)	3/3	3/3	2/2	2/2	10
Matematika	1	1	1	3	6
Fyzika	-	1	-	1	2
Technická angličtina	-	-	-	1	1
ODBORNÉ VZDELÁVANIE	**15**	**16**	**20**	**18**	**69**
Teoretické vzdelanie	6	9	8	9	32
Elektrotechnika	3/0	-	-	-	3
Elektronika	-	3/1	3/1	-	6
Elektrotechnické merania	-	-	-	3/2	3
Operačné systémy	-	3/2	-	-	3
Sieťové technológie	3/2	2/2	2/2	3/2	10
Finančná gramotnosť	-	-	-	2/0	2
Web	-	-	2/2	-	2
Kybernetická bezpečnosť	-	1/0	-	1/0	2
IKT – ešte určiť názov d)	-	-	1/0	-	1
KBZ – kryptografia d)	-	-	1/0	-	1
Praktická príprava	9	3	7	2	21
Robotika	2/2	-	-	-	2
Technické kreslenie	2/0	-	-	-	2
Prax	3/3	3/3	3/3	-	9
Aplikovaná informatika	2/2	-	-	-	2
Serverové technológie	-	-	2/2	2/2	4
PC architektúra	-	-	2/0	-	2
Disponibilné hodiny	0	4	5	7	16
Sieťové technológie	-	-	1/0	1/0	2
Programovanie	-	2/2	-	-	2
Databázové aplikácie	-	2/2	-	-	2

IKT – programovanie d)	-	-	2/2	2/2	4
IKT – databázové aplikácie d)	-	-	2/2	2/2	4
KBZ – penetračné testovanie d)	-	-	2/2	2/2	4
KBZ – sieťová bezpečnosť a etický hacking d)	-	-	2/2	2/2	4
Ročníkový projekt	-	-	-	1/1	1
Elektrotechnická spôsobilosť	-	-	-	1/0	1
Spolu	34	35	34	33	136
Účelové kurzy/učivo					
Lyžiarsky kurz	1	-	-	-	1
Kurz pohybových aktivít v prírode	1	-	-	-	1
Kurz na ochranu života a zdravia	-	-	1	-	1
Účelové cvičenie	1	1	-	-	1
Maturitná skúška	-	-	-	1	1

Poznámky k rámcovému učebnému plánu pre 4-ročné študijné odbory:

- Súčasťou vzdelávacej oblasti „Človek a hodnoty“ sú predmety náboženská výchova v alternatíve s etickou výchovou.
- Predmet informatika sa vyučuje v rámci odborných predmetov ako aplikovaná informatika.
- Druhý cudzí jazyk sa vyučuje ako voliteľný predmet z časovej dotácie disponibilných hodín v alternatíve nemecký jazyk s ruským jazykom v rámci disponibilných hodín v rozsahu 3 vyučovacích hodín v 1. a 2. ročníku a v rozsahu 2 vyučovacích hodín v 3. a 4. ročníku.
- V 3. ročníku žiak vyberá jedno zo zameraní:
  - IKT (špecialista informačných a komunikačných technológií) alebo
  - KBZ (špecialista kybernetickej bezpečnosti)

Za SPŠJM sme navrhovali predmet Kybernetická bezpečnosť nasledovne:

- V 2. ročníku 1 hodina teória s celou triedou.
- V 3. ročníku 5 hodín z toho 1 hodina teória s celou triedou a 4 hodiny cvičení v dvoch skupinách.
- V 4. ročníku 5 hodín z toho 1 hodina teória s celou triedou a 4 hodiny cvičení v dvoch skupinách. Vo vašom návrhu chýba zapracovanie 2 hodiny cvičení „Sieťová bezpečnosť“.

Vo vašom návrhu chýba zapracovanie 2 hodiny cvičení „Sieťová bezpečnosť“.

Obsahom predmetu Sieťová bezpečnosť by okrem iného mohla byť aj certifikácia Cisco Security alebo Fortinet.

Učebné osnovy jednotlivých predmetov

Predmet: Kybernetická bezpečnosť

Implementovaním vzdelávania kybernetickej bezpečnosti v odborných školách sa pripravujú odborníci, ktorí budú schopní nielen identifikovať a riešiť kybernetické hrozby, ale aj predchádzať potenciálnym rizikám a zvyšovať celkovú odolnosť technologických systémov. Tento vzdelávací smer reaguje na aktuálne potreby trhu práce, ktorý si vyžaduje kvalifikovaných profesionálov s odbornými znalosťami v oblasti kybernetickej bezpečnosti. Vzdelávanie v tejto oblasti preto podporuje nielen rozvoj technologických a analytických schopností, ale aj etického a zodpovedného prístupu k ochrane dát, čo je nevyhnutné pre budúcu profesionalitu a adaptabilitu mladých ľudí v dynamicky sa vyvíjajúcej digitálnej spoločnosti.

V nasledovných tabuľkách prinášame predmet kybernetická bezpečnosť pre stredné školy.

Odbor	2561 M Informačné a sieťové technológie
Časová dotácia	2. ročník – 1 hodina/týždeň 3. ročník – 5 hodín/týždeň 4. ročník – 5 hodín/týždeň
Forma štúdia	Denná
Vyučovací jazyk	Slovenský

Obsah výučby vychádza zo Štátneho vzdelávacieho programu pre odbor 25 Informačné a komunikačné technológie. Výučba je organizovaná nasledovne:

• 3. ročník: 1 hod. teória a 4 hod. cvičenia,

• 4. ročník: 1 hod. teória a 4 hod. cvičenia.

Cvičenia sa uskutočňujú v špecializovanej učebni a trieda je rozdelená na dve skupiny podľa predpisov MŠ SR.

Predmet *Kybernetická bezpečnosť* dopĺňa a rozširuje vedomosti z predmetov ako bezpečnosť sieťových technológií, operačných systémov a programovanie o základy informačnej bezpečnosti. Cieľom predmetu je poskytnúť žiakom vedomosti a zručnosti v oblasti kybernetickej bezpečnosti, jej implementácie, kontroly a legislatívy v SR. Žiaci nadobudnú prehľad o ochrane osobného počítača a mobilných zariadení.

V 3. ročníku sa žiaci zameriavajú na základné princípy kybernetickej bezpečnosti a implementáciu bezpečnostných technológií. V 4. ročníku sa orientujú na samostatnú analýzu a riadenie informačnej bezpečnosti, s dôrazom na odstránenie zraniteľností a rizík. Žiaci sa naučia princípy kybernetickej bezpečnosti. Budú prirodzene používať Digitálnu identitu. Žiakom sa stane prirodzeným bezpečnostné správanie na sociálnych sieťach a budú obozretní pred útokmi sociálneho inžinierstva. Naučia sa odhaľovať manipulatívne techniky sociálneho inžinierstva. Žiaci nadobudnú znalosť o analýze a riadení zraniteľností a z nich vyplývajúcich hrozieb. Žiaci budú vedieť rozoznať a vyriešiť incidenty a zabezpečiť kontinuitu biznisu.

V 4. ročníku sa žiaci zameriavajú na bezpečnosť sietí a následne sa zameriavajú na rozvíjanie práce s novými technológie ako sú cloudy a systémy umelej inteligencie. V rámci práce budú žiaci schopní analyzovať riziká na definovaných systémoch a aplikáciách. Dôležitou súčasťou je poznanie žiakov, ako nachádzať a riešiť zraniteľností systémov a ich overenie v rozsahu poznania systému OWASP top 10.

Predmet rozvíja komunikačné zručnosti, logické myslenie a schopnosť efektívne riešiť problémy. Žiaci sú vedení k samostatnému štúdiu a používaniu odbornej terminológie v slovenskom aj anglickom jazyku.

Tabuľka č. 3 Kybernetická bezpečnosť – návrh rozpisu učiva pre 2. ročník

Obsah vzdelávania – návrh rozpisu učiva			
Rozpis učiva predmetu	**Ročník**	**Počet vyučovacích hodín za týždeň**	**Počet vyučovacích hodín za ročník**
Kybernetická bezpečnosť	**Druhý**	**1**	**33**
Teória – 1h/týždeň			33
1. Úvod do kybernetickej bezpečnosti			**6**
1.1. Základné pojmy 1.2. Princípy kybernetickej bezpečnosti 1.3. Digitálna identita 1.4. Čo sú dáta a informácie			2 2 1 1
2. Prejavy a typy kyberkriminality			**6**
2.1. Útoky sociálneho inžinierstva (Phishing, Cyberstalking) 2.2. Ochrana pred útokmi typu Phishing a Cyberstalking 2.3. Právna ochrana podľa legislatívy SR pri kyberkriminalite			2 2 2
3. Logovanie v aplikáciách a Cookies			**2**
4. Manažment informačnej politiky			**2**
4.1. Bezpečnostná stratégia vo firme			2
5. Architektúra, komponenty a náklady informačného systému			**2**
6. Riadenie aktív a zodpovednosti za aktíva			**3**
7. Klasifikácia informácií a aktív			**3**
8. Základná ochrana PC			**8**
8.1. Typy útokov na PC 8.2. Zraniteľnosti a implementovanie záplat 8.3. Bezpečná práca s internetovým prehliadačom 8.4. Súkromie v kybernetickom priestore			2 2 2 2
9. Ochrana mobilného telefónu			**4**
9.1. Dáta, ktoré je potrebné chrániť v mobilnom zariadení 9.2. Správa systému a aplikácií			2 2

Tabuľka č. 4 Kybernetická bezpečnosť – návrh rozpisu učiva pre 3. ročník

Obsah vzdelávania – návrh rozpisu učiva			
Rozpis učiva predmetu	**Ročník**	**Počet vyučovacích hodín za týždeň**	**Počet vyučovacích hodín za ročník**
Kybernetická bezpečnosť	**tretí**	**5**	**165**
Teória – 1h/týždeň			33
1. Úvod do kryptografie			**4**
1.1. História kryptografie a základné pojmy a definície 1.2. Klasické šifrovacie metódy (Caesarova šifra, Vigenèrova šifra)			2 2
2. Symetrická kryptografia			**7**
2.1. Základné princípy symetrickej kryptografie 2.2. Blokové šifry (DES, AES) 2.3. Prúdové šifry (RC4) 2.4. Režimy šifrovania (ECB, CBC, CFB, OFB)			2 2 2 1
3. Asymetrická kryptografia			**6**
3.1. Základné princípy asymetrickej kryptografie 3.2. RSA algoritmus 3.3. Eliptické krivky 3.4. Diffie-Hellman výmena kľúčov			1 1 2 2
4. Kryptografické hash funkcie			**4**
5. Digitálne podpisy a certifikáty			**2**
6. Kryptografické protokoly			**2**
7. Aplikácia kryptografie			**4**
8, Typy útokov			**4**
8.1. DDoS 8.2. Malware			2 2
Cvičenie – 4h/týždeň			132
1. Princípy informačnej bezpečnosti			**4**
2. Kryptografia a elektronický podpis			**20**
2.1. Symetrické šifry 2.2. Asymetrické šifry 2.3. Hashovacie funkcie 2.4. Elektronický podpis 2.5. Aplikácia kryptografie 2.6. Kvantová a postkvantová kryptografia			4 4 2 2 2 2

3. Virtualizácia sieťových zariadení	**12**
3.1. Rozdelenie sieťových zariadení, podľa zamerania 3.2. Virtualizácia prepínačov a smerovačov 3.3. Modelovanie siete a prepojenie s virtuálnymi OS	4 4 4
4. Ochrana aplikácií a logovanie	**4**
5. Zabezpečenie LAN siete	**16**
5.1. Analýza komunikácie 5.2. Zabezpečenie sieťových prvkov 5.3. Jedntlivé typy útokov v prostredí sietí	8 4 4
6. Zabezpečenie WLAN	**12**
1. Šifrovacie protokoly (WEP, WPA, WPA2, WPA3) 2. Konfigurácia prístupových bodov 3. Konfigurácia WiFi Controler	4 4 4
7. Konfigurácia sieťových bezpečnostných prvkov	**14**
7.1. Konfigurácia a správa firewallov 7.2. Intrusion Detection Systems (IDS) 7.3. Intrusion Prevention Systems (IPS)	4 4 4
8. Zabezpečenie PC	**16**
8.1. Inštalácia PC 8.2. Bezpečnosť hesie, MFA a zdieľanie 8.3. Nastavenie základnej ochrany (lokálny FW, antivírus) 8.4. Riadenie používateľov a prístup na externé služby 8.5. Identifikovanie nepotrebných služieb a ich vypínanie 8.6. Nastavenie automatického patch managementu 8.7. Hardening OS na základe odporúčaní CIS katalógu	4 2 2 2 2 2 2
9. Ochrana servera	**16**
9.1. Inštalácia servera 9.2. Nastavenie základnej ochrany (lokálny FW, antivírus) 9.3. Riadenie používateľov 9.4. Nastavenie automatického patch managementu 9.5. Hardening podľa CIS catalógu 9.6. VPN a IPSec	6 2 2 2 2 2
10. Zabezpečenie komunikácie cez internet	**4**
10.1. Sniffing siete a identifikovanie nešifrovanej komunikácie 10.2.Nastavenie šifrovania pre vybrané služby	2 2

11. Incident management	**10**
11.1. Monitorovanie a detekcia hrozieb 11.2. Centrálne riadenie logov, inštalácia SIEM (Wazuh) 11.3. Odhaľovanie incidentov 11.4. Prehľadávanie a analýza logovacích záznamov	2 4 2 2
12. Kontinuita biznisu	**4**
12.1. Vytvorenie biznis kontinuity dokumentu 12.2. Spustenie incidentu a náprava podľa dokumentu	2 2

Tabuľka č. 5 Kybernetická bezpečnosť – návrh rozpisu učiva pre 4. ročník

Obsah vzdelávania – návrh rozpisu učiva			
Rozpis učiva predmetu	**Ročník**	**Počet vyučovacích hodín za týždeň**	**Počet vyučovacích hodín za ročník**
Kybernetická bezpečnosť	**štvrtý**	**3**	**150**
Teória – 1h/týždeň			30
1. Právne požiadavky v informačnej bezpečnosti			**8**
1.1. Základné pojmy a zákony 1.2. Prejavy kyber kriminality 1.3. Trestný zákon a legislatíva z pohľadu kybernetickej bezpečnosti 1.4. Autorský zákon			2 2 2 2
2. Ochrana nastavenia Cloudu			**16**
2.1. Čo je to cloud 2.2. Typy cloudu 2.3. Bezpečnostné prvky cloudu 2.4. Riziká cloudu			4 6 4 3
3. Systémy umelej inteligencie			**6**
3.1. Práca s umelou inteligenciou 3.2. Zber informácií (reconnaissance), analýza cieľov a identifikácia zraniteľností 3.3. Skenovanie a analýza zraniteľností			2 2 2
Cvičenie – 4h/týždeň			120
1. Techniky analýzy bezpečnosti IKT systémov			**18**
1.1. Testovanie zraniteľností 1.2. Techniky analýzy – pasívne 1.3. Techniky analýzy – aktívne 1.4. Odstraňovanie nálezov			4 4 4 4

2. Zraniteľnosť sietí	**12**
2.1. Zraniteľnosť LAN 2.2. Zraniteľnosť VAN 2.3. Zraniteľnosť Bluetooth a IoT	4 4 4
3. Penetračné testovanie	**40**
3.1. Etické a právne aspekty 3.2. Aplikačné zraniteľnosti 3.3. Zber informácií, analýza cieľov a identifikácia zraniteľností 3.4. Softvérové skenovanie a analýza zraniteľností 3.5. OWASP TOP 10 3.6. Bránenie zneužitia zraniteľností (exploitation)	4 4 8 8 12 4
4. Zraniteľnosť mobilných systémov a IoT	**4**
5. Požiadavky na bezpečný vývoj	**28**
5.1. Ochrana proti zraniteľnostiam a kontroly 5.2. Šifrovanie komunikácie 5.3. Správna autentifikácia a autorizácia 5.4. Bezpečnosť na úrovni dizajnu aplikácie 5.5. SAST a SBOM	4 4 4 8 8
7. Manažment rizík	**18**
7.1. Čo je to riziko 7.2. Identifikovanie rizík vo svojom okolí a v IKT systémoch 7.3. Odhadnutie rizika 7.4. Životný cyklus rizika 7.5. Práca s reziduálnym rizikom	4 16 4 2 2

Predmet: Operačné systémy

Zahrnutie kybernetickej bezpečnosti do predmetu Operačné systémy je nevyhnutné z dôvodu úzkeho prepojenia medzi týmito dvoma oblasťami a neustále sa zvyšujúcich bezpečnostných požiadaviek v digitálnom prostredí. Operačné systémy predstavujú základnú platformu, na ktorej beží všetok softvér a spracovávajú sa všetky dáta, čím sa stávajú cieľom kybernetických útokov. V rámci vzdelávania v oblasti operačných systémov je preto nevyhnutné zahrnúť aj kľúčové aspekty kybernetickej bezpečnosti, aby študenti získali nielen teoretické, ale aj praktické zručnosti v zabezpečovaní týchto systémov pred rôznymi hrozbami.

Operačné systémy sú miestom, kde sa riadia prístupové práva k systémovým a užívateľským dátam, spravujú sa sieťové pripojenia, inštalujú sa aplikácie a realizujú sa rôzne administratívne operácie. Bez adekvátnej bezpečnostnej ochrany môže byť každý z týchto procesov zneužitý na realizáciu škodlivých aktivít, ako sú neautorizovaný prístup, šírenie malwaru, zneužitie zraniteľností či únik citlivých informácií.

Zahrnutím tém kybernetickej bezpečnosti do výučby operačných systémov sa zabezpečí, že študenti budú schopní efektívne identifikovať potenciálne bezpečnostné riziká, implementovať ochranné opatrenia, ako je šifrovanie dát, správne nastavenie prístupových práv a kontrolu sieťovej komunikácie. Týmto spôsobom si študenti rozvinú praktické schopnosti potrebné na zabezpečenie operačných systémov v reálnych pracovných podmienkach a budú pripravení čeliť výzvam, ktoré kladie moderné digitálne prostredie.

Integrácia kybernetickej bezpečnosti do predmetu Operačné systémy tak nie je len reakciou na aktuálne bezpečnostné výzvy, ale aj investíciou do budúcej bezpečnosti technológií, na ktorých je postavená celá digitálna infraštruktúra.

V nasledovných tabuľkách prinášame návrh úprav pre predmet Operačné systémy pre stredné školy.

Odbor	2561 M Informačné a sieťové technológie
Časová dotácia	2. ročník – 3 hod./týždeň (z toho 2 hod. cvičení)
Forma štúdia	Denná
Vyučovací jazyk	Slovenský

Obsah výučby predmetu vychádza zo ŠVP pre odbor 25 Informačné a komunikačné technológie pre vyššie odborné vzdelávanie a je realizovaný v 2. ročníku štúdia. Vyučovanie zahŕňa jednu hodinu teoretickej výučby a dve hodiny cvičení, ktoré sa uskutočňujú v špecializovanej učebni a sú organizované v skupinách podľa predpisov MŠ SR. Cieľom predmetu je poskytnúť žiakom základné vedomosti o fungovaní operačných systémov, vrátane ich štruktúry, modulov a správy systémových prostriedkov.

V teoretickej časti sa študenti oboznamujú so spôsobmi správy operačných systémov a zabezpečenia údajov na úrovni súborového systému. Praktická časť sa zameriava na inštaláciu a konfiguráciu operačných systémov MS Windows a Linux, vrátane konfigurácie systémových a používateľských prostredí v sieťovom prostredí a pochopenie ako sa nastavuje bezpečný systém podľa zásad kybernetickej a informačnej bezpečnosti a nastavenie systému s vysokou mierou ochrany.

Predmet rozvíja zručnosti a vedomosti, ktoré súvisia s matematikou, fyzikou, elektrotechnikou a automatizáciou, a pripravuje študentov na ich využitie v odbornom vzdelávaní a praxi. Dôraz sa kladie na celoživotné vzdelávanie a profesijnú zodpovednosť. Témy sú rozšírené o princípy finančnej gramotnosti v oblasti licencovania operačných systémov.

Cieľom vyučovania je podporiť samostatnosť, tvorivosť a cieľavedomosť žiakov, pričom učiteľ motivuje, vedie a podporuje ich aktivitu, najmä v oblasti študijného odboru.

Tabuľka č. 6 Operačné systémy – návrh rozpisu učiva operačné systémy pre 2. ročník

Obsah vzdelávania – rozpis učiva			
Rozpis učiva predmetu	**Ročník**	**Počet vyučovacích hodín za týždeň**	**Počet vyučovacích hodín za ročník**
Operačné systémy	**druhý**	**3**	**99**
Teória - 1h/týždeň			33
1. Úvod do operačných systémov			**7**
2. Technické vybavenie počítača			**6**
3. Inštalácia OS			**4**
4. Správa OS			**12**

5. Vybraný operačný systém	**4**
Cvičenie - 2h/týždeň	66
1. Virtualizácia systému a inštalácia	**12**
2. Nastavenie operačného systému	**8**
3. Správa účtov a skupín v operačnom systéme	**10**
3.1. Lokálny užívatelia a skupiny 3.2. Riadenie oprávnení 3.3. Správa hesiel a autentifikácia	2 4 4
4. Bezpečnosť v OS	**10**
4.1. Bezpečnosť hesiel 4.2. Lokálny firewall 4.3. Minimálne požiadavky na zabezpečenie systému 4.4. Implementovanie záplat 4.5. Hardening OS (podľa CisCatalog)	2 4 4 2 2
5. Príkazový riadok	**10**
6. Špecifiká vybraného OS	**16**
… 6.2. Bezpečná komunikácia systémov Linux a Win a Mac OS	10 6

Predmet: Odborná prax

Predmet Odborná prax je veľmi ťažké správne rozšíriť o jednotlivé časti, ktoré nadväzujú na kybernetickú a informačnú bezpečnosť. Dôvodom je, že predmet je úzko spojený so zameraním školy a jednotlivými odbornými predmetmi, ktoré sa na strednej škole vyučujú. Nami navrhovaný predmet Odborná prax korešponduje s obsahom učiva na stredne škole so zameraním na elektrotechniku. Predpokladáme, že každá jednotlivé škola má predmet Odborná prax vytvorený a je v jeho kompetencii rozšíriť ho o nami navrhnuté body. Prvý ročník je zameraný na odborné predmety nesúvisiace s kybernetickou a informačnou bezpečnosťou. Druhý ročník vytvára prostredie na pochopenie dôležitosti bezpečnosti PC a dôležitosti riadenia účtov v operačnom systéme. V treťom ročníku sa bezpečnosť zameria na bezpečný vývoj a vytvorenie návykov na bezpečný vývoj softvéru.

V nasledovných tabuľkách prinášame návrh úprav pre predmet Operačné systémy pre stredné školy.

Odbor	2561 M Informačné a sieťové technológie
Časová dotácia	1. ročník – 3 hod./týždeň 2. ročník – 3 hod./týždeň 3. ročník – 3 hod./týždeň
Forma štúdia	Denná
Vyučovací jazyk	Slovenský

Obsah výučby predmetu prax vychádza zo vzdelávacej oblasti „Odborné vzdelávanie“ v rámci ŠVP 25 Informačné a sieťové technológie. Prax sa organizuje v skupinách, pričom trieda je rozdelená do dvoch alebo troch pracovísk.

Cieľom je spojenie teoretických vedomostí s praktickou činnosťou, pričom dôraz je kladený na získanie zručností pri výbere vhodných materiálov, nástrojov a technologických postupov pri výrobe zariadení. Žiaci sa vedú k samostatnému a tvorivému technickému mysleniu, aplikácii teoretických poznatkov v praxi a dodržiavaniu bezpečnosti pri práci a ochrany životného prostredia.

V rámci osvojovania technologických postupov sa žiaci učia vybrať vhodné nástroje a najefektívnejší výrobný proces, pričom sa zameriavajú na moderné technológie v elektrotechnike a elektronike. V bezpečnosti sa žiaci zamerajú na riadenie prístupov a bezpečný vývoj. Prax sa vykonáva v školských dielňach a odborných učebniach, kde žiaci realizujú cvičné a produktívne práce, ako montáž a nastavovanie elektronických zariadení. Hlavným cieľom je rozvíjať zručnosti v diagnostike, údržbe a prevádzke zložitých elektronických systémov.

Od prvého ročníka sú žiaci oboznámení so zásadami bezpečnosti práce, ochranou zdravia, rizikami úrazov a zásadami prvej pomoci pri úraze elektrickým prúdom. Finančná gramotnosť je súčasťou praktických cvičení, pričom sa kladie dôraz na zodpovedné hospodárenie s ohľadom na životné prostredie a potreby výroby, prevádzky a údržby elektrotechnických zariadení.

Tabuľka č. 7 Odborná prax – návrh rozpisu učiva operačné systémy pre 1. ročník

Obsah vzdelávania – rozpis učiva			
Rozpis učiva predmetu	**Ročník**	**Počet vyučovacích hodín za týždeň**	**Počet vyučovacích hodín za ročník**
Prax	**prvý**	**3**	**99**
1. Ručné a strojové obrábanie			**33**
1.1. Meradlá, náradie 1.2. Opracovanie materiálu			9 24
2. Elektroinštalácia			**33**
2.1. Úvod 2.2. Prenosová a spojovacia technika 3.3. Zapojenie inštalácie			9 9 15
3. Spájkovanie			**33**
3.1. Elektronické súčiastky 3.2. Spájkovanie vodičov a pasívnych súčiastok			12 21

Tabuľka č. 8 Odborná prax – návrh rozpisu učiva operačné systémy pre 2. ročník

Obsah vzdelávania – rozpis učiva			
Rozpis učiva predmetu	**Ročník**	**Počet vyučovacích hodín za týždeň**	**Počet vyučovacích hodín za ročník**
Prax	**druhý**	**3**	**99**
1. PC hardware and software			**50**
1.1. PC hardware … *Mobilné zariadenia* **1.2. PC software a služby** … *Ochrana PC a jednotlivých služieb* **1.3. Riadenie prístupov** *Používateľských* *Aplikačných* *Administrátorských*			**28** 6 **16** 5 **6** 2 2 2
2. Návrh a výroba plošných spojov chýba obsah vzdelávania			**49**

Tabuľka č. 9 Odborná prax – návrh rozpisu učiva operačné systémy pre 3. ročník

Obsah vzdelávania – rozpis učiva			
Rozpis učiva predmetu	**Ročník**	**Počet vyučovacích hodín za týždeň**	**Počet vyučovacích hodín za ročník**
Prax	**tretí**	**3**	**99**
1. WEB			**50**
1.1. Vybraný jazyk používaný pri tvorbe web prostredia … *Pravidlá a podmienky bezpečného vývoja* **1.2. Skriptovanie na strane klienta** **1.3. Individuálny projekt**			**22** 2 **14** **12**
2. Programovanie v sieťach			**49**
2.1. Základné programovanie v objektovom jazyku … *Bezpečné programovanie: SBOM a SAST* **2.2. Aplikácie skriptovacieho programovacieho jazyka** **2.3. Aplikácie objektového programovacieho jazyka**			**16** 3 6 **20** **13**

Predmet: Serverové technológie

Predmet serverové technológie sa zameriava na správu a riadenie najrozšírenejších operačných systémov Linux a Windows a nastavenie základnej bezpečnosti v rámci systémov. Vzdelávanie v oblasti kybernetickej bezpečnosti pri vyučovaní správy operačných systémov Linux a Windows je kľúčové, pretože oba tieto systémy sú často cieľom kybernetických útokov a ich správna konfigurácia a zabezpečenie sú nevyhnutné pre ochranu údajov a systémov.

Operačné systémy, ako Linux a Windows, sú základom IT infraštruktúry, a preto sa stávajú zraniteľnými voči rôznym hrozbám, ako sú vírusy, malvér, útoky typu ransomware, neoprávnený prístup alebo zneužitie systémových zraniteľností. Pre správu týchto systémov je nevyhnutné, aby administrátori mali nielen technické zručnosti v oblasti inštalácie a konfigurácie, ale aj dôkladné znalosti bezpečnostných opatrení, ktoré chránia operačný systém pred týmito hrozbami.

Kybernetická bezpečnosť pri správe operačných systémov zahŕňa rôzne aspekty, ako je nastavenie správnych prístupových práv, šifrovanie dát, monitoring systémových logov, implementácia firewallov a iných ochranných nástrojov, ako aj správne zálohovanie dát. Bez adekvátnej bezpečnostnej stratégie môže byť systém zraniteľný a vystavený rôznym hrozbám, ktoré môžu viesť k úniku citlivých informácií alebo k poškodeniu dát.

Vzdelávanie v tejto oblasti zabezpečuje, že administrátori operačných systémov budú schopní efektívne identifikovať a riešiť bezpečnostné problémy, správne nastaviť ochranné mechanizmy a reagovať na potenciálne hrozby, čím sa minimalizuje riziko škodlivých útokov a zaručuje bezpečná prevádzka systémov. Tým sa zvyšuje bezpečnosť organizácie a ochraňuje sa jej digitálna infraštruktúra.

V nasledovných tabuľkách prinášame návrh úprav pre predmet Serverové technológie pre stredné školy.

Odbor	2561 – M informačné a sieťové technológie
Časová dotácia	3. ročník – 2 hod./týždeň 4. ročník – 2 hod./týždeň
Forma štúdia	Denná
Vyučovací jazyk	Slovenský
Obsah výučby vychádza zo Štátneho vzdelávacieho programu pre odbor 25 Informačné a komunikačné technológie. Výučba v 3. a 4. ročníku je organizovaná formou 2 hodín cvičení týždenne, pričom trieda je rozdelená do skupín podľa predpisov MŠ SR a cvičenia prebiehajú v špecializovanej učebni. Predmet Serverové technológie rozširuje učivo z predmetu *Operačné systémy* a zameriava sa na správu počítačových systémov, operačných systémov a počítačových sietí. Obsah zahŕňa architektúru počítačových systémov, sieťový hardvér a základnú konfiguráciu sieťových zariadení. Pri tvorbe učiva bol dôraz kladený na praktickú aplikáciu poznatkov v správe serverových systémov a poskytovaní serverových služieb podľa modelu klient-server. Predmet sa zameriava na správu serverového hardvéru a softvéru, vrátane využívania dokumentácie svetových výrobcov. Žiaci sa oboznámia s odbornou terminológiou v slovenskom aj anglickom jazyku. Výučba prebieha na výkonných počítačoch s operačnými systémami a virtualizačnými nástrojmi v kvalitne vybavenej učebni. V rámci predmetu sa rozvíja aj finančná gramotnosť formou hodnotenia technologických riešení v oblasti serverových systémov, pričom sa zohľadňuje efektívnosť vynaložených nákladov na zabezpečenie kvality.	

Tabuľka č. 10 Serverové technológie – návrh rozpisu učiva operačné systémy pre 3. ročník

Obsah vzdelávania – rozpis učiva			
Rozpis učiva predmetu	**Ročník**	**Počet vyučovacích hodín za týždeň**	**Počet vyučovacích hodín za ročník**
Operačné systémy Linux a Windows	**tretí**	**2**	**66**
1. Inštalácia a základná konfigurácia OS Windows server			**10**
2. Riadenie serverových služieb			**14**
3. Správa Active Directory			**12**
3.1. Správa administrátorských a doménových účtov 3.2. Správa používateľských účtov …			2 2
4. Správa ukladacieho priestoru a zálohovanie			**12**
4.1. Nastavenie zálohovania ako ochrany pred malware …			2
5. Sieťová komunikácia v rámci OS Windows server			**8**
6. Bezpečnosť OS Windows server			**10**
6.1 Logovanie v OS Windows 6.2 Modelovanie zraniteľností v OS Windows 6.3 Nastavovanie multifaktorovej autentifikácie 6.4 Riadenie prevádzkového softvéru, záplaty			2 4 2 2

Tabuľka č. 11 Serverové technológie – návrh rozpisu učiva operačné systémy pre 4. ročník

Obsah vzdelávania – rozpis učiva			
Rozpis učiva predmetu	**Ročník**	**Počet vyučovacích hodín za týždeň**	**Počet vyučovacích hodín za ročník**
Serverové technológie	**štvrtý**	**2**	**60**
1. Základy Linuxu			**10**
2. Správa OS Linux			**16**
2.1. Správa používateľských účtov 2.2 Správa administrátorských účtov …			2 2
3. Sieťové služby v OS Linux			**12**
4. Serverové služby v OS Linux			**8**

…	4
4.2. Služby bezpečného pripojenia na server	4
5. Bezpečnosť OS Linux	**14**
5.1 Riadenie prevádzky	2
5.2 Ochrana proti Malware	2
5.3 Zálohovanie	4
5.4 Logovanie	2
5.5 Hardening OS podľa CisCatalog	4

Záver

Návrh predmetov, ktoré sme rozširovali je nastavený tak, aby stredné odborné školy mali možnosť rozšírenia zakomponovať do svojich predmetov a nie výlučne sa musia držať názvov predmetov tak ako sme ich navrhli. Z toho dôvodu sme obsah jednotlivých odborných predmetov definovali na odborné kapitoly a nerozpisovali sme ich viac. Rozpísané sú len časti, ktoré sa venujú kybernetickej bezpečnosti. Tieto časti následne je možné zgrupovať a vkladať do iných odborných predmetov vzhľadom na zameranie školy. Dôležitým predmetom pri vzdelávaní bezpečnosti sú sieťové technológie. Tento predmet je v súčasnosti na školách zvyčajne dobre uchopený a preto ho v rámci našej štúdie nerozpisujeme, ale predpokladáme jeho existenciu.

Implementáciou jednotlivých častí informačnej a kybernetickej bezpečnosti do vzdelávacieho programu dosiahneme výchovu nielen odborných kapacít, ktoré sú zamerané na funkčnosť systémov a prevádzku. Bude pre nich dôležitá aj bezpečnosť systémov a kontinuita biznisu.

NORMATÍV MATERIÁLOVO-TECHNICKÉHO ZABEZPEČENIA

Pre inováciu študijného odboru 2561 M Informačné a sieťové technológie odporúčame doplniť aktuálny normatív materiálovo-technického zabezpečenia pre tento študijný odbor o učebné priestory pre praktické vyučovanie zamerané na kybernetickú bezpečnosť a to nasledovné učebne:

- Učebňa kybernetickej bezpečnosti a penetračného testovania
- Učebňa sieťovej bezpečnosti

1. Základné údaje

Normatív materiálno-technického a priestorového zabezpečenia (ďalej len „normatív“) je vytvorený s cieľom zabezpečenia kvalitnej prípravy absolventov študijného odboru 2561 M informačné a sieťové technológie. Normatív vychádza zo Štátneho vzdelávacieho programu

(ďalej len „ŠVP“) pre skupinu odborov 26 Elektrotechnika o poskytujúceho úplné stredné odborné vzdelanie. Špecifikuje ucelený, vzájomne sa podmieňujúci komplex požiadaviek s cieľom vytvoriť optimálne vzdelávacie prostredie.

Normatív určuje požiadavky na základné učebné priestory a požiadavky na základné vybavenie učebných priestorov pre teoretické a praktické vyučovanie v študijnom 2561 M Informačné a sieťové technológie.

Okrem základných priestorov a základného vybavenia sú súčasťou normatívu aj odporúčané učebné priestory a odporúčané materiálno-technické a prístrojové vybavenie. Tieto sú nad rámec základného vybavenia, ich účelom je zabezpečenie vyššej kvality vyučovacieho procesu v nadväznosti na požiadavky trhu práce v danom odbore.

Vybavenosť v súlade s normatívom v rozsahu odporúčaného vybavenia je predpokladom pre strednú odbornú školu uchádzať sa o možnosť pôsobiť ako centrum odborného vzdelávania a prípravy.

2. Všeobecne záväzné právne predpisy

Proces výchovy a vzdelávania zohľadňuje všeobecne záväzné právne predpisy upravujúce bezpečnosť práce, ochranu pred požiarom, prevádzkovanie objektov škôl a školských zariadení ako aj technickú dokumentáciu používaných zariadení, príslušné normy a predpisy, ktoré upravujú výrobný proces alebo pracovné operácie zodpovedajúce obsahu vzdelávania v danom odbore vzdelávania.

Učebné priestory musia vyhovovať požiadavkám hygieny práce, bezpečnosti a ochrane zdravia pri práci, ochrany pred požiarom, ktoré sú v súlade s príslušnými platnými všeobecne záväznými právnymi predpismi, rezortnými predpismi a technickými normami. Priestory, v ktorých sa uskutočňuje teoretické a praktické vyučovanie musia umožňovať optimálnu organizáciu vyučovania s prihliadnutím na technický rozvoj a zavádzanie nových zariadení do prevádzky.

Súčasťou vybavenia učebných priestorov pre praktické vyučovanie je technická dokumentácia, technologické postupy, pravidlá bezpečnej obsluhy technických a iných zariadení, hygienické a bezpečnostné predpisy, bezpečnostné tabuľky a značky a prostriedky protipožiarnej ochrany a prvej pomoci.

3. Základné učebné priestory

Základné učebné priestory sú nevyhnutné na nadobudnutie požadovaných vedomostí a zručností stanovených výkonovými štandardami príslušného ŠVP a špecifík výučby študijného odboru 2694 M Informačné a sieťové technológie.

Počet, rozmery a vybavenie šatní a hygienických zariadení – umyvární, spŕch, WC musia byť navrhnuté v súlade s typologickými a typizačnými smernicami, normami STN EN, hygienickými normami, predpismi o bezpečnosti a ochrane zdravia pri práci, predpismi o ochrane požiarom platnými pre normovanie a prevádzku zariadení pre prípravu žiakov na povolanie.

Priestory pre teoretické vyučovanie uvedené v tabuľke č. 12 a priestory pre praktické vyučovanie uvedené v tabuľke č. 13 musia vyhovovať všeobecne záväzným právnym predpisom.

3.1. Základné učebné priestory pre teoretické vyučovanie

Tabuľka č. 12 Názov učebného priestoru pre teoretické vyučovanie

P. č.	Názov učebného priestoru pre teoretické vyučovanie
1.	Učebňa pre výučbu elektrotechniky a aplikovanej elektroniky
2.	Učebňa pre výučbu softvérových technológií
3.	Učebňa pre výučbu hardvérových technológií

3.2. Základné učebné priestory pre praktické vyučovanie

Tabuľka č. 13 Názov učebného priestoru pre praktické vyučovanie

P. č.	Názov učebného priestoru pre praktické vyučovanie
1.	Učebňa elektrotechniky a aplikovanej elektroniky
2.	Učebňa programovania a databázových technológií
3.	Učebňa operačných systémov a serverových technológií
4.	Učebňa sieťových technológií
5.	Učebňa robotiky
6.	Učebňa IT architektúr a servisných platforiem
7.	Učebňa odbornej praxe pre informačné technológie
8.	Učebňa odbornej praxe pre elektrotechniku
9.	Učebňa odbornej praxe sieťových prvkov

4. Základné vybavenie učebných priestorov

Jednotlivé učebné priestory pre teoretické a praktické vyučovanie uvedené v tretej časti sú rozpracované v tabuľkách č. 14 a č. 15, kde je uvedené základné vybavenie pre teoretické vyučovanie a základné vybavenie pre praktické vyučovanie v danom odbore. Pri vybavení pracovného miesta žiaka sú uvedené všetky základné pomôcky, náradie a pod., ktoré žiak potrebuje v procese teoretickej a praktickej prípravy vo svojom odbore vrátane osobných ochranných pracovných prostriedkov.

Pre všetky položky označené „podľa potreby“ sa nedá presne vyšpecifikovať množstvo, ale pre daný študijný odbor sú povinné, jedná sa najmä o materiálne vybavenie učebných priestorov, potrebný materiál, ktorý musí byť stále k dispozícii a názorné učebné pomôcky.

4.1. Základné vybavenie učebných priestorov pre teoretické vyučovanie

Tabuľka č. 14 Základné vybavenie učebných priestorov pre teoretické vyučovanie

Teoretické vyučovanie			
P. č. a názov priestoru (z tab. č. 12)	**Názov vybavenia**	**Počet na**	
		žiaka	**skupinu**
1. Učebňa pre výučbu elektrotechniky a aplikovanej elektroniky	Pracovný stôl pre učiteľa		1
	Pracovný stôl (miesto) pre žiaka	1	
	Stolička kancelárska		1
	Stolička školská	1	
	Tabuľa/keramická tabuľa		1
	Prezentačná plocha/interaktívna tabuľa s dataprojektorom s ultrakrátkou projekčnou vzdialenosťou		1
	PC zostava (notebook) pre učiteľa + softvér *1, 2*		1
	Sieť LAN		1
	Vizualizér s ohybným kĺbom		1
	Multifunkčné laserové zariadenie (sieťové)		1
	Hlasovacie zariadenie	1	
	Prepojovací materiál (konektory, káble…)		podľa potreby
	Programové a didaktické vybavenie pre elektrotechniku a elektroniku		podľa potreby
	Skrine na odkladanie pomôcok pre výučbu		podľa potreby
2. Učebňa pre výučbu softvérových technológií	Pracovný stôl pre učiteľa		1
	Pracovný stôl (miesto) pre žiaka	1	
	Stolička kancelárska		1
	Stolička školská	1	
	Tabuľa/keramická tabuľa		1
	Prezentačná plocha/interaktívna tabuľa s dataprojektorom s ultrakrátkou projekčnou vzdialenosťou		1
	PC zostava (notebook) pre učiteľa + softvér *1, 2, 3, 6*		1
	PC zostava (notebook) + softvér *1, 2, 3, 6*	1	
	Sieť LAN		1
	Vizualizér s ohybným kĺbom		1

2. Učebňa pre výučbu softvérových technológií	Multifunkčné laserové zariadenie (sieťové)		1
	Hlasovacie zariadenie	1	
	Programové a didaktické vybavenie pre programovanie a operačné systémy		podľa potreby
	Skrine na odkladanie pomôcok pre výučbu		podľa potreby
3. Učebňa pre výučbu hardvérových technológií	Pracovný stôl pre učiteľa		1
	Pracovný stôl (miesto) pre žiaka	1	
	Stolička kancelárska		1
	Stolička školská	1	
	Tabuľa/keramická tabuľa		1
	Prezentačná plocha/interaktívna tabuľa s dataprojektorom s ultrakrátkou projekčnou vzdialenosťou		1
	PC zostava (notebook) pre učiteľa + softvér *1, 2, 3, 6*		1
	Server		1
	Sieť LAN		1
	Vizualizér s ohybným kĺbom		1
	Multifunkčné laserové zariadenie (sieťové)		1
	Hlasovacie zariadenie	1	
	Programové a didaktické vybavenie pre operačné systémy a serverové technológie		podľa potreby
	Skrine na odkladanie pomôcok pre výučbu		podľa potreby
	Skrine na odkladanie pomôcok pre výučbu		podľa potreby

4.2. Základné vybavenie učebných priestorov pre praktické vyučovanie

Tabuľka č. 15 Základné vybavenie učebných priestorov pre praktické vyučovanie

Praktické vyučovanie			
P. č. a názov priestoru (z tab. č. 13)	**Názov vybavenia**	**Počet na**	
		žiaka	**skupinu**
1. Učebňa pre výučbu elektrotechniky a aplikovanej elektroniky	Pracovný stôl pre učiteľa		1
	Pracovný stôl (miesto) pre žiaka	1	
	Stolička kancelárska		1
	Stolička školská	1	

1. Učebňa pre výučbu elektrotechniky a aplikovanej elektroniky	Tabuľa/keramická tabuľa		1
	Prezentačná plocha/interaktívna tabuľa s dataprojektorom s ultrakrátkou projekčnou vzdialenosťou		1
	PC zostava (notebook) pre učiteľa + softvér *1, 2*		1
	Sieť LAN		1
	Vizualizér s ohybným kĺbom		1
	Multifunkčné laserové zariadenie (sieťové)		1
	Simulačné programy pre elektrotechniku a elektroniku		podľa potreby
	Univerzálny merací prístroj (U, I, W, R, L, C, f, cos Φ)	2	
	Napájací zdroj jednosmerného a striedavého napätia	1	
	Generátor		5
	Osciloskop		5
	Logický analyzátor		5
	Čítač		5
	Súprava pasívnych a aktívnych elektronických prvkov		podľa potreby
	Súprava základných logických obvodov		podľa potreby
	Prepojovací materiál (konektory, káble…)		podľa potreby
	Skrine na odkladanie meracej techniky a pomôcok		podľa potreby
2. Učebňa programovania a databázových technológií	Pracovný stôl pre učiteľa		1
	Pracovný stôl (miesto) pre žiaka	1	
	Stolička kancelárska		1
	Stolička školská	1	
	Tabuľa/keramická tabuľa		1
	Prezentačná plocha/interaktívna tabuľa s dataprojektorom s ultrakrátkou projekčnou vzdialenosťou		1
	PC zostava (notebook) pre učiteľa + softvér *1, 2, 3, 6*		1
	PC zostava (notebook) + softvér *1, 2, 3, 6*	1	
	Sieť LAN		1
	Multifunkčné laserové zariadenie (sieťové)		1

2. Učebňa programovania a databázových technológií	Vývojové prostredie pre programovanie v jazykoch napr. C++, Java, …		podľa potreby
	Vývojové prostredie pre programovanie databáz napr. MS SQL, MySQL, Oracle…		podľa potreby
	Skrine na odkladanie didaktickej techniky a pomôcok		podľa potreby
3. Učebňa operačných systémov a serverových technológií	Pracovný stôl pre učiteľa		1
	Pracovný stôl (miesto) pre žiaka	1	
	Stolička kancelárska		1
	Stolička školská	1	
	Tabuľa/keramická tabuľa		1
	Prezentačná plocha/interaktívna tabuľa s dataprojektorom s ultrakrátkou projekčnou vzdialenosťou		1
	PC zostava (notebook) pre učiteľa + softvér *1, 2, 4, 5*		1
	PC zostava (notebook) + softvér *1, 2, 4, 5*	1	
	Sieť LAN		1
	Server		1
	Multifunkčné laserové zariadenie (sieťové)		1
	Skrine na odkladanie didaktickej techniky a pomôcok		podľa potreby
4. Učebňa sieťových technológií	Pracovný stôl pre učiteľa		1
	Pracovný stôl (miesto) pre žiaka	1	
	Stolička kancelárska		1
	Stolička školská	1	
	Tabuľa/keramická tabuľa		1
	Prezentačná plocha/interaktívna tabuľa s dataprojektorom s ultrakrátkou projekčnou vzdialenosťou		1
	PC zostava (notebook) pre učiteľa + softvér *1, 2, 7*		1
	PC zostava (notebook) + softvér *1, 2, 7*	1	
	Tester sietí		1
	Sieť LAN		1
	Multifunkčné laserové zariadenie (sieťové)		1
	Cvičná zostava na konfiguráciu sieťových zariadení (napr. Cisco, MikroTik)		5

4. Učebňa sieťových technológií	Cvičná konfiguračná sada na WiFi *		5
	Skrine na odkladanie didaktickej techniky a pomôcok		podľa potreby
5. Učebňa robotiky	Pracovný stôl pre učiteľa		1
	Pracovný stôl (miesto) pre žiaka	1	
	Stolička kancelárska		1
	Stolička školská	1	
	Tabuľa/keramická tabuľa		1
	Prezentačná plocha/interaktívna tabuľa s dataprojektorom s ultrakrátkou projekčnou vzdialenosťou		1
	PC zostava (notebook) pre učiteľa + softvér *1, 2, 8*		1
	PC zostava (notebook) + softvér *1, 2, 8*	1	
	Sieť LAN		1
	Multifunkčné laserové zariadenie (sieťové)		1
	Stavebnica robota (napr. LEGO Education)	1	
	Skrine na odkladanie didaktickej techniky a pomôcok		podľa potreby
6. Učebňa IT architektúr a servisných platforiem	Pracovný stôl pre učiteľa		1
	Pracovný stôl (miesto) pre žiaka	1	
	Stolička kancelárska		1
	Stolička školská	1	
	Tabuľa/keramická tabuľa		1
	Prezentačná plocha/interaktívna tabuľa s dataprojektorom s ultrakrátkou projekčnou vzdialenosťou		1
	PC zostava (notebook) pre učiteľa + softvér *1, 2*		1
	PC zostava (notebook) + softvér *1, 2*	1	
	Sieť LAN		1
	Vizualizér s ohybným kĺbom		1
	Multifunkčné laserové zariadenie (sieťové)		1
	PC zostava na servis *	1	
	Sada učebných pomôcok pre výučbu PC architektúr		podľa potreby
	Skrine na odkladanie didaktickej techniky a pomôcok		podľa potreby

7. Učebňa odbornej praxe pre informačné technológie	Pracovný stôl pre učiteľa		1
	Pracovný stôl (miesto) pre žiaka	1	
	Stolička kancelárska		1
	Stolička školská	1	
	Tabuľa/keramická tabuľa		1
	Prezentačná plocha/interaktívna tabuľa s dataprojektorom s ultrakrátkou projekčnou vzdialenosťou		1
	PC zostava (notebook) pre učiteľa + softvér *1, 2*		1
	PC zostava na servis, inštaláciu *	1	
	Sieť LAN		1
	Multifunkčné laserové zariadenie (sieťové)		1
	Sada učebných pomôcok pre výučbu PC architektúr		
	Montážny materiál pre IT architektúru (napr. sada skrutiek, napäťových, dátových káblov)	1	
	Súprava náradia pre IT	1	
	Skrine na odkladanie didaktickej techniky a pomôcok		podľa potreby
8. Učebňa odbornej praxe pre elektrotechniku	Pracovný stôl pre učiteľa		1
	Pracovný stôl (miesto) pre žiaka	1	
	Stolička kancelárska		1
	Stolička školská	1	
	Tabuľa/keramická tabuľa		1
	Prezentačná plocha/interaktívna tabuľa s dataprojektorom s ultrakrátkou projekčnou vzdialenosťou		1
	PC zostava (notebook) pre učiteľa + softvér *1, 2*		1
	Súprava náradia pre elektrotechniku (kombinované kliešte, skrutkovač plochý, skrutkovač krížový, ihlové pilníky, pinzeta, odstraňovač izolácie, odsávačka cínu a iné)	1	
	Mikrospájkovačka	1	
	Multimeter (U, I, R, L, C)	2	
	Logická sonda	1	
	Laboratórny zdroj		5
	Generátor		5

8. Učebňa odbornej praxe pre elektrotechniku	Osciloskop		5
	Logický analyzátor		5
	Čítač		5
	Súprava pasívnych a aktívnych elektronických prvkov		podľa potreby
	Súprava základných logických obvodov		podľa potreby
	Skrine na odkladanie didaktickej techniky a pomôcok		podľa potreby
9. Učebňa odbornej praxe sieťových prvkov	Pracovný stôl pre učiteľa		1
	Pracovný stôl (miesto) pre žiaka	1	
	Stolička kancelárska		1
	Stolička školská	1	
	Tabuľa/keramická tabuľa		1
	Prezentačná plocha/interaktívna tabuľa s dataprojektorom s ultrakrátkou projekčnou vzdialenosťou		1
	PC zostava (notebook) pre učiteľa + softvér *1, 2*		1
	PC zostava (notebook) + softvér *1, 2*	1	
	Súprava náradia pre štrukturovanú kabeláž (krimpovacie kliešte, kombinované kliešte, štípacie kliešte skrutkovače a iné)	1	
	Laboratórny zdroj		1
	Generátor signálov do 200 MHz		1
	Osciloskop		1
	Logický analyzátor		1
	Čítač		1
	Multimeter		2
	Tester káblových dátových systémov		5
	Skrine na odkladanie didaktickej techniky a pomôcok		podľa potreby

1) Softvér pre priamu interakciu učiteľa a žiaka, umožňuje zdieľanie obsahu obrazovky učiteľského počítača na počítači žiaka, kontrolu a ovládanie počítača žiaka učiteľom (napr. LanSchool)

2) Softvér umožňujúci zachovanie nakonfigurovaných systémových a aplikačných nadstavení. Správa softvéru cez LAN, WAN alebo internet. Znemožňuje inštaláciu nežiaduceho softvéru do počítača. Možnosť tichej inštalácie klientov priamo od administrátora z jedného miesta (napr. Deep Freeze)

3) Programové vybavenie umožňujúce výučbu programovacích jazykov vyššej generácie – multilicencia. Programovací jazyk na princípe „byte-code", ktorý nie je závislý na konkrétnej platforme, viacparadigmový programovací jazyk pre objektovo orientované programovanie, ale aj generické programovanie.

4) Programové vybavenie učebne pozostávajúce z najmenej dvoch nezávislých serverových platforiem, ktoré sú aktuálne štatisticky najviac používané v praxi. Multilicencia pre celú učebňu, ktorá obsahuje dvoje platformy a zároveň aj príslušné licenčné vybavenie zabezpečujúce serverové prostredie, virtualizáciu a cloud computing.

5) Programové vybavenie učebne pozostávajúce z najmenej dvoch nezávislých operačných systémov – platforiem, ktoré sú aktuálne štatisticky najviac používané v praxi. Multilicencia pre celú učebňu, ktorá obsahuje dvoje platformy a zároveň aj príslušné licenčné vybavenie pre aplikačné programy. Licencia na antivírusové vybavenie.

6) Programové vybavenie učebne pozostávajúce z najmenej štyroch programov na tvorbu a spracovanie relačných databáz, databázových serverov, ale aj platformu na využitie dát pomocou Business Intelligence (BI). Použitie platforiem, ktoré sú aktuálne štatisticky najviac používané v praxi. Multilicencia pre celú učebňu.

7) Programové vybavenie učebne pre sieťové technológie, pozostávajúce z multilicencie (napr. CISCO alebo Mikrotik sieťovej akadémie) e-learningové prostredie.

8) Vývojové prostredie pre robotizáciu pozostávajúce z robotických sad a príslušného softvéru (napr. Lego Education)

**) Zariadenie určené pre praktickú výučbu na rozoberanie, skladanie, konfiguráciu*

5. Odporúčané učebné priestory

Zriadenie odporúčaných učebných priestorov pre zabezpečenie teoretického a praktického vyučovania umožní realizovať kvalitnejšiu výučbu vzhľadom na požiadavky školského vzdelávacieho programu v študijnom odbore 2694 M Informačné a sieťové technológie.

5.1. Odporúčané učebné priestory pre teoretické vyučovanie

Tabuľka č. 16 Odporúčané učebné priestory pre teoretické vyučovanie

P. č.	Názov učebného priestoru pre teoretické vyučovanie
1.	Multimediálna učebňa

5.2. Odporúčané učebné priestory pre praktické vyučovanie

Tabuľka č. 17 Odporúčané učebné priestory pre praktické vyučovanie

P. č.	Názov učebného priestoru pre praktické vyučovanie
1.	Učebňa mobilných a webových technológií
2.	Učebňa WiFi
3.	Učebňa kybernetickej bezpečnosti a penetračného testovania
4.	Učebňa sieťovej bezpečnosti

6. Odporúčané vybavenie učebných priestorov

Uvedené odporúčané vybavenie učebných priestorov umožní realizovať kvalitnejšiu teoretickú aj praktickú výučbu, ktorá poskytuje kompetencie nad rámec profilu absolventa.

6.1. Odporúčané vybavenie učebných priestorov pre teoretické vyučovanie

Tabuľka č. 18 Odporúčané vybavenie učebných priestorov pre teoretické vyučovanie

Teoretické vyučovanie			
P. č. a názov priestoru (z tab. č. 16)	**Názov vybavenia**	**Počet na**	
		žiaka	**skupinu**
1. Multimediálna učebňa	Pracovný stôl pre učiteľa		1
	Pracovný stôl (miesto) pre žiaka	1	
	Stolička kancelárska		1
	Stolička školská	1	
	Tabuľa/keramická tabuľa		1
	Prezentačná plocha/interaktívna tabuľa s dataprojektorom s ultrakrátkou projekčnou vzdialenosťou		1
	PC zostava (notebook) pre učiteľa + softvér *1, 2*		1
	PC zostava (notebook) + softvér *1, 2*	1	
	Sieť LAN		1
	Vizualizér s ohybným kĺbom		1
	Multifunkčné laserové zariadenie (sieťové)		1
	Hlasovacie zariadenie	1	1
	Skrine na odkladanie didaktickej techniky a pomôcok		podľa potreby

6.2. Odporúčané vybavenie učebných priestorov pre praktické vyučovanie

Tabuľka č. 19 Odporúčané vybavenie učebných priestorov pre praktické vyučovanie

Praktické vyučovanie			
P. č. a názov priestoru (z tab. č. 17)	**Názov vybavenia**	**Počet na**	
		žiaka	**skupinu**
1. Učebňa mobilných a webových technológií	Pracovný stôl pre učiteľa		1
	Pracovný stôl (miesto) pre žiaka	1	
	Stolička kancelárska		1
	Stolička školská	1	

1. Učebňa mobilných a webových technológií	Prezentačná plocha + dataprojektor		1
	PC zostava (notebook) pre učiteľa + softvér *1, 2*		1
	PC zostava (notebook) + softvér *1, 2*	1	
	Sieť LAN		1
	Tlačiareň (sieťová pre viac učební)		1
	Súprava náradia pre servis výpočtovej techniky		podľa potreby
	Vývojové prostredie pre programovanie mobilných technológií		podľa potreby
	Vývojové prostredie pre programovanie webových technológií		podľa potreby
	WiFi karta do PC		podľa potreby
	Prepojovací materiál (konektory, káble…)		podľa potreby
	Skrine na odkladanie didaktickej techniky a pomôcok		podľa potreby
2. Učebňa WiFi	Pracovný stôl pre učiteľa		1
	Pracovný stôl (miesto) pre žiaka	1	
	Stolička kancelárska		1
	Stolička školská	1	
	Prezentačná plocha + dataprojektor		1
	PC zostava (notebook) pre učiteľa + softvér *1, 2, 7*		1
	PC zostava (notebook) + softvér *1, 2, 7*	1	
	Sieť LAN		1
	Tlačiareň (sieťová pre viac učební)		1
	Aktívne a pasívne prvky WiFi siete (router, switch, bridge, AP, antény, …)		podľa potreby
	Rack - serverová skriňa		podľa potreby
	Sieťový server s pripojením na Internet		1
	WiFi karta do PC		podľa potreby
	Súprava náradia pre servis výpočtovej techniky		podľa potreby

2. Učebňa WiFi	Prepojovací materiál (konektory, káble…)		podľa potreby
	Skrine na odkladanie didaktickej techniky a pomôcok		podľa potreby
3. Učebňa kybernetickej bezpečnosti a penetračného testovania	Interaktívna dotyková tabuľa		1
	Rack - serverová skriňa		1
	Reálna LAN sieť: - kabeláž, zásuvky - Switch pripojený do školskej siete		1
	Cvičná LAN sieť: - kabeláž, zásuvky - manažovateľný Switch na vytvorenie oddelenej siete - cvičný hardvérový Server na simuláciu útokov s OS napr. Windows Server 2019		1
	Výkonný počítač: - dva monitory (na prácu s viacerými VM nutné!) - CPU: min. i7 - RAM: min. 32 GB - SSD: systém 512 GB, dáta min. 2 TB - sieťová karta LAN - OS: Windows Enterprise	1	
	Server na spúšťanie virtuálnych strojov pre žiakov (napr. Vmware ESXi)		1
	NAS dátové úložisko		1
	Operačný systém Kali Linux spušťaný ako VM	1	
	Operačný systém Parrot Security OS spúšťaný ako VM	1	
	Simulačné nástroje: - Cisco Packet Tracer - GNS3 - EVE-NG	1	
	Bezpečnostné nástroje: - Wireshark (analýza sieťového prenosu). - Metasploit Framework. - Nessus, OpenVAS (zraniteľnosti). - Hashcat (lámacie nástroje na heslá)	1	
	Šifrovacie a certifikačné nástroje: - OpenSSL, Keytool, Certbot	1	
	SIEM nástroje: - Splunk, Graylog alebo ELK Stack (monitorovanie udalostí)		1
	Súprava náradia pre servis výpočtovej techniky		podľa potreby

3. Učebňa kybernetickej bezpečnosti a penetračného testovania	Prepojovací materiál (konektory, káble…)		podľa potreby
	Skrine na odkladanie didaktickej techniky a pomôcok		podľa potreby
4. Učebňa sieťovej bezpečnosti	Interaktívna dotyková tabuľa		1
	Rack - serverová skriňa		1
	Reálna LAN sieť: - kabeláž, zásuvky - Switch pripojený do školskej siete		1
	Cvičná LAN sieť: - kabeláž, zásuvky - manažovateľný Switch na vytvorenie oddelenej siete - cvičný hardvérový Server na simuláciu útokov s OS napr. Windows Server 2019 - hardvérový Firewall napr. Cisco ASA		1
	Výkonný počítač: - dva monitory - CPU: min. i7 - RAM: min. 32 GB - SSD: systém 512 GB, dáta min. 2 TB - sieťová karta LAN - sieťová kartqa WiFi - konektor RS232 na pripojenie DB9-RJ45 konzolového kábla - OS: Windows Enterprise	1	
	WiFi AccessPoint	1	
	Simulačné nástroje: - Cisco Packet Tracer - GNS3 - EVE-NG	1	
	Bezpečnostné nástroje: - Wireshark (analýza sieťového prenosu). - Metasploit Framework. - Nessus, OpenVAS (zraniteľnosti). - Hashcat (lámacie nástroje na heslá)	1	

7. Požiadavky na učebné priestory a ich vybavenie pre všeobecnovzdelávacie predmety

7.1. Základné učebné priestory

Tabuľka č. 20 Základné učebné priestory

P. č.	Názov učebného priestoru pre praktické vyučovanie
1.	Učebňa
2.	Telocvičňa

7.2. Základné vybavenie učebných priestorov

Tabuľka č. 21 Základné vybavenie učebných priestorov

P. č. a názov priestoru (z tab. č. 20)	Názov vybavenia (v členení stroje a zariadenia, prístroje, výpočtová technika, nábytok a pod.)	Počet na	
		žiaka	skupinu
1. Učebňa	Katedra		1
	Stolička	1	
	Školská lavica	1	
	Školská tabuľa s kresliacimi pomôckami		1
	Skriňa		1
	Učebné pomôcky (podľa predmetov)		1
	Nástenka		1
2. Telocvičňa	Rebrina		8
	Tyč na šplhanie		2
	Lano na šplhanie		2
	Kruhy		1
	Hrazda		1
	Lavička		6
	Karimatka	1	
	Žinenka		6
	Švihadlo	1	
	Švédska debna		2
	Koza		1
	Odrazový mostík		1
	Volejbalová konštrukcia		1
	Volejbalová sieť		1
	Volejbalová lopta		8
	Basketbalová konštrukcia s doskou a košom		2
	Basketbalová lopta		8
	Futbalová/hádzanárska brána		2

2. Telocvičňa	Futbalová lopta		8
	Stopky		1
	Meracie pásmo		1
	CD (DVD) prehrávač s reproduktormi		1
	Učebné pomôcky (obrazový materiál, videozáznamy, dataprojektor, počítač, netradičné náčinie a i. podľa potrieb výučby)		1
	Skrinka pre audiovizuálnu techniku		1

7.3. Odporúčané učebné priestory

Kvalitnejšiu výučbu v danom odbore umožní zriadenie odporúčaných nadštandardných učebných priestorov pre zabezpečenie vyučovania všeobecnovzdelávacích predmetov. Odporúčané (nadštandardné) učebné priestory zriaďuje škola podľa potreby na základe vlastných priestorových a ekonomických možností.

Tabuľka č. 22 Odporúčané učebné priestory pre praktické vyučovanie

P. č.	Názov učebného priestoru pre praktické vyučovanie
1.	Fyzikálna učebňa
2.	Jazyková učebňa
3.	Multimediálna učebňa
4.	Matematická učebňa

7.4. Odporúčané vybavenie učebných priestorov

Tabuľka č. 23 Odporúčané vybavenie učebných priestorov

P. č. a názov priestoru (z tab. č. 22)	Názov vybavenia (v členení stroje a zariadenia, prístroje, výpočtová technika, nábytok a pod.)	Počet na	
		žiaka	skupinu
1. Fyzikálna učebňa	Pracovný stôl pre učiteľa		1
	Stolička	1	
	Pracovný stôl pre žiaka	1	
	Skriňa		1
	Interaktívna tabuľa		1
	Učebné pomôcky (podľa potrieb výučby)		1
	Dataprojektor		1

1. Fyzikálna učebňa	Notebook	1	
	Notebook/stolový počítač		1
	Prístup na internet	1	
	Zdroj napätia a prúdu		1
	USB kľúč		2
	Indukčný varič		1
	Súprava pre časť mechanika – demonštračná súprava		1
	Súprava pre časť mechanika – žiacka súprava	1	
	Súprava pre časť termodynamika – demonštračná súprava		1
	Súprava pre časť termodynamika – žiacka súprava	1	
	Súprava pre časť optika – demonštračná súprava		1
	Súprava pre časť optika – žiacka súprava	1	
	Lekárnička		1
	Súprava pre časť elektrina – demonštračná súprava		1
	Súprava pre časť elektrina – žiacka súprava	1	
	Súprava pre časť magnetizmus – demonštračná súprava		1
	Súprava pre časť magnetizmus – žiacka súprava	1	
2. Jazyková učebňa	Katedra		1
	Stolička	1	
	Školská lavica	1	
	Školská tabuľa s kresliacimi pomôckami		1
	Skriňa		1
	Interaktívna tabuľa		1
	Učebné pomôcky (podľa potrieb výučby)		1
	Nástenka		1
	Dataprojektor		1
	Notebook	1	
	Notebook/stolový počítač		1
	CD prehrávač/DVD prehrávač *		1

2. Jazyková učebňa	Slúchadlá	1	
	Prístup na internet	1	
	USB kľúč		2
3. Multimediálna učebňa	Katedra		1
	Stolička	1	
	Školská lavica	1	
	Školská tabuľa s kresliacimi pomôckami		1
	Skriňa		1
	Interaktívna tabuľa		1
	Učebné pomôcky (podľa potrieb výučby)		1
	Nástenka		1
	Dataprojektor		1
	Notebook/stolový počítač	1	
	Reproduktory **		2
	Multifunkčné zariadenie		3
	USB kľúč	1	
	Kamera		1
	Prístup na internet	1	
	Veľkoplošný TV 3 D + DVD		1
4. Matematická učebňa	Katedra		1
	Stolička	1	
	Školská lavica	1	
	Školská tabuľa s kresliacimi pomôckami		1
	Skriňa		1
	Interaktívna tabuľa		1
	Magnetická tabuľa		1
	Učebné matematické pomôcky a rysovacie pomôcky (podľa potrieb výučby)		1
	Nástenka		1
	Dataprojektor		1

4. Matematická učebňa	Notebook/stolový počítač		1
	Notebook	1	
	Prístup na internet	1	
	Matematický softvér		1
	USB kľúč		2
	Čítacie zariadenie (kamera)		1

** Prípadne iný audio systém podľa potrieb a ekonomických možností školy.*

*** V prípade, že nie sú integrované v rámci PC.*

IDENTIFIKÁCIA PRÍLEŽITOSTÍ VZDELÁVANIA (ŠKÔL A ZAMESTNÁVATEĽOV) V OBLASTI KYBERNETICKEJ BEZPEČNOSTI

Na riešenie akútneho nedostatku kvalifikovanej pracovnej sily v oblasti kybernetickej bezpečnosti je cieľom vzdelávania v navrhovanom inovovanom študijnom odbore 2561 M Informačné a sieťové technológie pripraviť v relatívne krátkom čase špecialistov pre oblasť kybernetickej bezpečnosti. Trendom je neustály nárast dopytu po odborníkoch, ktorý je daný najmä neustálym vývojom hrozieb kybernetickej bezpečnosti a stále prísnejšími legislatívnymi opatreniami na ochranu osobných údajov a kybernetickej bezpečnosti. Organizácie musia spĺňať rôzne bezpečnostné štandardy a nariadenia, čo významne zvyšuje dopyt po odborníkoch, ktorí budú vykonávať implementáciu a dodržiavanie týchto pravidiel.

Zavádzanie opatrení kybernetickej bezpečnosti si vyžaduje odborne zdatný a kvalifikovaný personál, ktorí pozná informačné technológie, dokáže vytvoriť bezpečnú architektúru, identifikovať relevantné bezpečnostné hrozby a stanoviť adekvátne protiopatrenia na ich elimináciu.

Inovovaný študijný odbor je dostatočne široko odborne zameraný a univerzálny. Poskytuje východisko na ďalšiu kariérnu špecializáciu. Pre absolventov prichádza do úvahy užšia špecializácia na konkrétnu oblasť kybernetickej bezpečnosti podľa požiadaviek, alebo potrieb zamestnávateľa.

Vzdelávacie inštitúcie, ktoré by mali poskytovať vzdelávanie a prípravu v tomto študijnom odbore musia spĺňať podmienku garancie kvality vzdelávania a prípravy a podmienku prepojenia s praxou, pretože oblasť kybernetickej bezpečnosti je v neustálom vývoji. Zdokonaľujú sa ako prístupy a technologické platformy tak aj techniky a taktiky útočníkov zameraných na škodlivé aktivity. Náročné materiálovo-technické a technologické zázemie pre kvalitnú výučbu je finančne náročné no je nevyhnutné. Preto je potrebná spolupráca s privátnou sférou či už formou spolupráce s lokálnymi spoločnosťami, alebo nadnárodnými spoločnosťami pôsobiacim v oblasti kybernetickej bezpečnosti , ktoré majú za týmto účelom zavedené globálne programy. Okrem spolupráce s privátnym sektorom je nevyhnutná aj spolupráca s verejným sektorom najmä s v oblasti aktívnej podpory formou výziev z rôznych programov ako Plán obnovy a odolnosti SR[25], alebo Program Slovensko 2021 – 2027[26].

Príprava absolventov by mala byť koncentrovaná na školách so dostatočnou praxou a odbornými kompetenciami v to proporcionálne v rámci všetkých regiónov. Povinnosti regulácie kybernetickej bezpečnosti bude nevyhnutné aplikovať na všetky povinné organizácie na celom území Slovenskej republiky. Z tohto dôvodu je potreba kvalifikovanej pracovnej sily celoslovenská.

Z pohľadu náročnosti na zdroje je vhodné aby bola realizovaná aj spolupráca so zamestnávateľmi v oblasti kybernetickej bezpečnosti. Za rovnako významnú považujeme spoluprácu záujmovými združeniami, alebo mimovládnymi organizáciami ktoré sa venujú oblasti kybernetickej bezpečnosti a združujú špičkových odborníkov v tejto oblasti.

Je taktiež potrebné venovať pozornosť na rozvoj budúcnosti vzdelávania a kumuláciu odborného potenciálu pre vyučovanie problematiky kybernetickej bezpečnosti. Koncentrácia odborníkov, investícií, prostriedkov a energie do väčších a odborne pripravených vzdelávacích inštitúcií dáva vyššiu šancu na ich ďalší rozvoj a spoluprácu so sektormi.

Na základe špecifikovaných požiadaviek na inováciu ako aj dlhodobých skúseností s implementáciou študijného odboru 2561 M Informačné a sieťové technológie boli identifikované stredné priemyselné školy, kde je potenciál prípravy absolventov v tomto inovovanom študijnom odbore.

Tabuľka č. 24 Identifikácia príležitostí vzdelávania

P. č.	Škola	Mesto	Ulica	Webové sídlo
1.	Stredná priemyselná škola Jozefa Murgaša	Banská Bystrica	Hurbanova 6	https://spsjm.sk/

2.	Stredná priemyselná škola elektrotechnická Karola Adlera	Bratislava	Karola Adlera 5	https://www.adlerka.sk/
3.	Stredná priemyselná škola elektrotechnická	Bratislava	Hálova 16	https://spsehalova.sk/
4.	Stredná priemyselná škola	Stará Turá	Športová 675	http://www.sosst.sk/zsse/
5.	Stredná priemyselná škola	Púchov	Školská 715/2	https://www.spojskola-pu.sk/
6.	Stredná priemyselná škola elektrotechnická S. A. Jedlika	Nové Zámky	Komárňanská 28	www.spojenaskolanz.edupage.org
7.	Stredná priemyselná škola informačných technológií	Kysucké Nové Mesto	Nábrežná 1325	www.spsknm.sk
8.	Stredná priemyselná škola elektrotechnická	Prešov	Plzenská 1	https://spse-po.sk/
9.	Stredná priemyselná škola elektrotechnická	Košice	Komenského 44	https://www.spseke.sk/
10.	Stredná priemyselná škola technická	Spišská Nová Ves	Štúrova 5	https://spst.sk/
11.	Stredná priemyselná škola	Považská Bystrica	Slov. partizánov 1132/52	https://www.spspb.sk/
12.	Stredná priemyselná škola technická	Martin	Ul. Ambra Pietra 10	https://spsmt.sk/

Všetky z vyššie uvedených stredných škôl v súčasnej dobe ponúkajú študijný odbor 2561 M Informačné a sieťové technológie.

Stredná priemyselná škola Jozefa Murgaša, Banská Bystrica ponúka študijný odbor 2561 M Informačné a sieťové technológie aj s čiastočne zapracovanou oblasťou kybernetickej bezpečnosti.

Veľmi významnú považujeme aj spoluprácu so záujmovými organizáciami a občianskymi združeniami, ktoré v súčasnej dobe vykonávajú značnú podpornú činnosť aj v oblasti stredných škôl. V nasledovnej tabuľke sú uvedené niektoré záujmové združenia a občianske združenia, ktoré aktívne pôsobia v oblasti kybernetickej bezpečnosti či už šírením osvety, alebo formou vykonávania a organizovania rôznych aktivít.

Tabuľka č.25 Záujmové organizácie a občianske združenia s potenciálom spolupráce na odbornom vzdelávaní a príprave

P. č.	Názov organizácie	Webové sídlo
1.	Preventista – združenie pre bezpečnosť a prevenciu	https://preventista.sk
2.	Cluster Kybernetickej Bezpečnosti	https://clusterkb.sk
3.	Nadácia ESET	https://www.nadaciaeset.sk
4.	Komunita kybernetickej bezpečnosti	https://www.kyberkomunita.sk/kyberkomunita/

Ako už bolo vyššie spomenuté pri vzdelávaní a príprave odborníkov na kybernetickú bezpečnosť je nevyhnutné spolupracovať aj s inštitúciami verejného sektora a vybranými vysokými školami. V súlade so prijatými stratégiami pre oblasť kybernetickej bezpečnosti sú vyvíjané aktivity na posilnenie kybernetickej odolnosti štátu.

Za účelom kontinuálneho zvyšovanie úrovne kybernetickej bezpečnosti sú jednotlivými inštitúciami verejnej správy vykonávané aktivity v oblasti definovania stratégie, legislatívnych návrhov, koordinácie a podpory, vzdelávania alebo medzinárodnej spolupráce. V neposlednom rade je to aj poskytovanie finančnej podpory projektom zameraným na zvyšovanie kybernetickej bezpečnosti vo verejnej správe a v súkromnom sektore.

Tabuľka č. 26 Zoznam organizácií verejnej správy a škôl s potenciálom spolupráce na odbornom vzdelávaní a príprave

P. č.	Názov organizácie	Webové sídlo
1.	Národný bezpečnostný úrad (NBÚ)	https://www.nbu.gov.sk/kyberneticka-bezpecnost/
2.	Kompetenčné a certifikačné centrum kybernetickej bezpečnosti	https://cybercompetence.sk/
3.	SK-CERT	https://www.sk-cert.sk/sk/o-nas/index.html
4.	Ministerstvo investícií, regionálneho rozvoja a informatizácie SR	https://mirri.gov.sk/sekcie/informatizacia/o-sekciach/kyberneticka-bezpecnost/
5.	CSIRT.sk	https://csirt.sk/
6.	CSIRT-UPJŠ	https://www.upjs.sk/pracoviska/ciakt/it-sluzby/22682-2/
7.	Žilinská univerzita v Žiline	https://www.uniza.sk/

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti bolo poverené plnením úloh Národného koordinačného centra v Slovenskej republike v zmysle nariadenia EÚ 2021/887[27], ktoré vytvorilo Európske kompetenčné centrum v oblasti kybernetickej bezpečnosti ECCC a sieť národných NCC. Národné koordinačné centrum Slovensko (NCC-SK) slúži ako jednotné kontaktné miesto pre podniky, firmy, organizácie, verejnú správu a širokú verejnosť. Spolupracujeme s Európskym kompetenčným centrom, európskou sieťou národných koordinačných centier ako aj inými medzinárodnými partnermi. ECCC a NCC boli vytvorené s cieľom posilniť kapacity a konkurencieschopnosť Európy v oblasti kybernetickej bezpečnosti a vytvoriť silnú Komunitu pre túto oblasť. Hlavným cieľom tejto iniciatívy je koordinovať aktivity v oblasti kybernetickej bezpečnosti na všetkých úrovniach v európskom prostredí.

ECCC a NCC sú tiež určené na zhromažďovanie investícií do výskumu, technológií a priemyselného rozvoja v oblasti kybernetickej bezpečnosti a na lepšiu koordináciu plánovania v rámci programov financovania EÚ Horizont Európa a Digitálna Európa.

Významným prínosom bolo aj spustenie výzvy[28] na vytvorenie kompetenčných centier kybernetickej bezpečnosti Ministerstvom investícií, regionálneho rozvoja a informatizácie (MIRRI).

Vytvorenie centier excelentnosti bude slúžiť v jednotlivých regiónoch (8 x VUC) a umožní študentom, pedagógom reálny dosah k moderným technológiám v rozsahu moderného hardware vybavenia a inovatívneho a pokrokového softwarového vybavenia určeného pre monitoring kybernetickej bezpečnosti. Pre vybrané stredné školy, v spolupráci s vysokými školami a komerčným sektorom, sa do tvorby centra zapoja najmä poskytnutím svojho know-how.

Vytvorenie centier spája (vytvára) prostredie k pravidelným stretnutiam a napomáha dosiahnutiu vzájomnej synergie. Získaním komplexného obrazu o činnostiach spojených s ochranou dátových aktív, členovia komunity získavajú predpoklady pre šírenie osvety (v oblasti kybernetickej bezpečnosti) aj na regionálnej úrovni, pri nadväzovaní kontaktov s inými vertikálami regiónu (stredné školy a pod.).

Žilinská univerzita v Žiline v súčasnej dobe poskytuje inovačné vzdelávanie[29] v oblasti kybernetickej bezpečnosti. Cieľom inovačného vzdelávania je prehĺbenie, rozšírenie a inovácia profesijných kompetencií potrebných na výkon pracovnej činnosti v príslušnej kategórii alebo v podkategórii pedagogického zamestnanca alebo v príslušnej kategórii odborného zamestnanca alebo uplatnenie najnovších poznatkov alebo skúseností z praxe vo výchove a vzdelávaní. Realizuje sa ako jednoduchý program inovačného vzdelávania v rozsahu najmenej 50 hodín. Ukončuje sa záverečnou prezentáciou pred trojčlennou komisiou.

V tejto súvislosti je však potrebné poznamenať, že stredné školy nedisponujú potrebnými zdrojmi, aby bolo možné zabezpečiť pedagogickým zamestnancov takúto formu ďalšieho vzdelávania. Z tohto dôvodu by bolo vhodné vytvorenie nástroja na financovanie vzdelávania pedagogických zamestnancov a tak zabezpečiť adekvátne kapacity pre zavedenie inovovaného študijného odboru.

V neposlednom rade je nevyhnutné vytvoriť priestor aj na možnosť zdieľania praktických skúseností vo vyučovacom procese pre špecialistov. Toto je možné dosiahnuť spoluprácou inštitúcií a spoločností, ktoré už dnes subjektmi regulovanými podľa zákona o kybernetickej bezpečnosti[30] najmä na regionálnej úrovni. Potreba špecialistov v tejto oblasti a udržateľnosti v regiónoch dáva týmto subjektom možnosť už vo výučbovom procese nájsť si vhodných kandidátov na neobsadené pozície, ktoré sa budú účinnosti novely zákona len zvyšovať.

Z hľadiska identifikácie spoločností, ktoré by mohli spolupracovať na zabezpečení odborného vzdelávania a prípravy ide najmä o tie, ktorých doména podnikania sú služby v oblasti kybernetickej bezpečnosti. Medzi spoločnosti s potencionálnom spolupráce boli identifikované spoločností, ktoré sa významne podieľajú na poskytovaní služieb kybernetickej bezpečnosti.

Tabuľka č. 27 Identifikácia spoločností s potenciálom spolupráce na odbornom vzdelávaní a príprave

P. č.	Názov spoločnosti	Webové sídlo
1.	ACCURA s.r.o.	https://www.accura.io/
2.	Alanata a. s.	https://www.alanata.sk/
3.	Aliter Technologies, a.s.	https://www.aliter.com/
4.	AXENTA s.r.o.	https://www.axenta.sk/
5.	Binary Confidence s.r.o.	https://www.binaryconfidence.com/
6.	board.sk, s.r.o.	https://www.board.sk/
7.	Citadelo	https://citadelo.com/sk
8.	Cyllium SK, s.r.o.	https://cyllium.eu/
9.	Datalan, a.s.	https://www.datalan.sk/
10.	DataTrend Services, s.r.o.	https://www.datatrendservices.sk/
11.	DITEC, a.s.	https://www.ditec.sk/

12.	ESET, spol. s r.o	https://www.eset.com/sk/
13.	exe, a. s.	https://www.exe.sk/
14.	GAMO a.s.	https://www.gamo.sk/
15.	InterWay, a. s.	https://www.interway.sk/
16.	Istrosec s.r.o.	https://istrosec.com/sk/
17.	ITSEN, s. r. o.	https://www.itsen.sk/
18.	KIOS a.s.	https://www.kios.sk/
19.	Kodiva, s.r.o.	https://kodiva.sk/
20.	KOLAS s. r. o.	https://www.kolas.sk/
21.	O2 Slovakia, s.r.o.	https://www.o2.sk/
22.	Orange Slovensko, a.s.	https://www.orange.sk/
23.	QuBit Security, s.r.o.	https://qubitconference.com/
24.	SOITRON S.R.O.	https://www.soitron.sk/
25.	Sicurio s.r.o.	https://www.sicurio.sk/
26.	Slovak Telekom, a.s.	https://www.telekom.sk/
27.	Slovanet, a. s.	https://biznis.slovanet.net/
28.	Deutsche Telekom IT Solutions Slovakia	https://www.deutschetelekomitsolutions.sk/
29.	VNET a.s.	https://www.vnet.sk/sk/
30.	void SOC, s.r.o.	https://voidsoc.com/

ANALÝZA POTENCIÁLU UPLATNENIA ABSOLVENTOV A IDENTIFIKÁCIA MOŽNÝCH CIEĽOVÝCH SKUPÍN ŽIAKOV A RODIČOV PRE OBLASŤ ŠTÚDIA KYBERNETICKEJ BEZPEČNOSTI

Technologický vývoj vo svete ide neustále dopredu. Sociálne siete, online transakcie, cloud computing a automatizované procesy poháňajú svet. Spolu s nimi však rastie aj kybernetická kriminalita, ktorá neustále vyvíja nové typy, nástroje a techniky útokov, ktoré útočníkom pomáhajú preniknúť do inak zložitých alebo dobre kontrolovaných prostredí a spôsobiť škody, a dokonca zostať neodhalení.

Na účely ochrany pred kybernetickými útokmi boli prijaté regulácie s cieľom zvýšenia kybernetickej bezpečnosti a odolnosti kľúčových subjektov a celých sektorov voči aktuálnym hrozbám. V novembri 2022 Európsky parlament aktualizoval právne predpisy EÚ s cieľom posilniť investície do silnej kybernetickej bezpečnosti základných služieb a kritickej infraštruktúry a posilniť pravidlá platné v celej EÚ. Parlament podporil tiež pravidlá zlepšujúce ochranu základnej infraštruktúry EÚ, vrátane digitálne infraštruktúry. Právne predpisy sprísňujú požiadavky na posudzovanie rizík a podávanie správ pre kritické subjekty v 11 základných odvetviach. Najvýznamnejšou reguláciou je napríklad smernica NIS2, ktorá zavádza prísnejšie požiadavky na kybernetickú bezpečnosť v kľúčových sektoroch. Počet regulovaných sektorov sa zväčšil, do regulácie kybernetickej bezpečnosti sa implementáciou smernice NIS2 dostali nové sektory, ktoré neboli dotknuté predchádzajúcou reguláciou. Jedná sa najmä o sektory ako výroba liekov, výroba zdravotníckych pomôcok, poštové a kuriérske služby, odpad a odpadové vody, verejná správa, výskum a vývoj, vesmírny sektor. Pre všetky uvedené sektory bude potrebné, aby prijali opatrenia na riadenie rizík v oblasti kybernetickej bezpečnosti.

V SR dňa 1. apríla 2018 nadobudol účinnosť zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti, čím zároveň do slovenského právneho poriadku transponuje európsku Smernicu o sieťovej a informačnej bezpečnosti (NIS). V súčasnej dobe nadobudla účinnosť od 1. januára 2025 novela zákona ako transpozícia Smernice NIS2. Existuje dôvodný predpoklad, že touto transpozíciou stúpne počet povinných subjektov niekoľkonásobne.

Tak, ako už bolo uvedené, odborníkov v oblasti kybernetickej bezpečnosti je nedostatok a podľa predpokladov sa ich nedostatok vo vzťahu k predmetnej novele ešte prehĺbi. Existuje teda spoločenská objednávka na odborníkov na kybernetickú bezpečnosť.

Zo zákona o kybernetickej bezpečnosti vyplýva povinným subjektom (prevádzkovateľom základnej služby) zákonná povinnosť mať zriadenú pozíciu manažéra kybernetickej bezpečnosti. Zákonom je upravená aj pozícia audítora kybernetickej bezpečnosti. Tým, že vzrastie počet auditovaných subjektov, požiadavka na zvýšenie ich počtu je viac než relevantná.

Je možné konštatovať, že z pohľadu strednodobého horizontu je v súčasnej dobe hodnotené ako efektívne kontinuálne vzdelávanie vo vzdelávacích inštitúciách, no z dlhodobého pohľadu je situácia riešená iba formou vysokoškolského vzdelávania.

Je preto nevyhnutné budovať systém vzdelávania v oblasti kybernetickej bezpečnosti, počnúc zvyšovaním bezpečnostného povedomia na základných školách, cez vytvorenie študijných odborov až po vysokoškolské vzdelávanie a pokryť tak chýbajúce odborné personálne kapacity na všetkých úrovniach.

Záverom komparatívnej analýzy tejto štúdie je návrh inovácie odboru 2561 M Informačné a sieťové technológie. Inovácia by mala byť navrhnutá formou zamerania využitím voliteľných predmetov pre 3. a 4 ročník, tak aby mal absolvent by mal po absolvovaní 2. ročníka možnosť výberu zamerania. Jedným zo zameraní by tak bol – Špecialista kybernetickej bezpečnosti.

Absolvent študijného odboru je kvalifikovaným odborníkom, ktorý má vedomosti a zručnosti v oblasti kybernetickej bezpečnosti serverov, sietí, koncových bodov, webových aplikácií, kryptografie, programovania, právnej výchovy a manažmentu bezpečnostných rizík, je zodpovedný za plnenie špecifických úloh v rámci svojej špecializácie v kybernetickej bezpečnosti.

Absolvent má kvalifikáciu na úrovni úplného stredného odborného vzdelania a môže vykonávať odborné činnosti v miestnych orgánoch štátnej správy a regionálnej samosprávy, ako aj v podnikateľských subjektoch, ale aj v subjektoch hospodárskej mobilizácie, či u prevádzkovateľov prvkov kritickej infraštruktúry.

Široký odborný profil s nevyhnutným všeobecným vzdelaním, s dostatočnou adaptabilitou, logickým myslením a schopnosťou aplikovať nadobudnuté vedomosti pri riešení problémov predpokladá uplatnenie absolventa v sektoroch Energetika, Doprava, Financie, Zdravotníctvo, Voda a atmosféra, Digitálna infraštruktúra, Riadenie služieb IKT (medzi podnikmi), Verejná správa, Vesmír. Je schopný čo najlepšie uplatniť štúdiom získané vedomosti, schopnosti a zručnosti v širšom spektre profesií a ďalej prakticky rozvíjať svoju osobnosť a zameranie činnosti. Absolvent by mal byť preto schopný neustále sa vzdelávať a sledovať vývoj a nové poznatky v oblasti kybernetickej bezpečnosti.

Potenciál uplatnenia absolventa vo vybraných profesiách podľa požiadaviek trhu práce

V súčasnej dobe, resp. ku dňu spracovania tejto štúdie, nie je možné jednoznačne zadefinovať zamestnanie, v ktorom by sa absolvent mal uplatniť, podľa Slovenského kvalifikačného rámca (SKKR), ktorý na základe vopred stanovených kritérií priraďuje určitú úroveň jednotlivým kvalifikáciám z Národnej sústavy kvalifikácií. Jednotlivé bezpečnostné role z oblasti kybernetickej bezpečnosti nie sú definované v Registri Národnej sústavy povolaní a nemajú vytvorenú príslušnú kartu kvalifikácií a prípadnú referenciu k Európskemu kvalifikačnému rámcu.

Napriek uvedenému, otázka poddimenzovania zamestnancov v oblasti kybernetickej bezpečnosti rezonuje na mnohých bezpečnostných fórach, odbornou verejnosťou, je témou konferencií, workshopov, odborných článkov i publikácií a nevyhnutnosť vzdelávania pre budovanie kybernetickej odolnosti je nevyhnutná.

Identifikácia možných cieľových skupín žiakov a rodičov pre oblasť štúdia kybernetickej bezpečnosti

Študijný odbor je charakteristický zameraním na aktuálne problémy v kyberpriestore. Štúdium kybernetickej bezpečnosti vyžaduje silné základy v IT, programovaní, počítačových sieťach, kryptografii a analýze hrozieb. Okrem technických znalostí je potrebné aj pochopenie právnych a etických aspektov a schopnosť reagovať na incidenty v reálnom čase. Profesionál v tejto oblasti musí byť schopný neustále sledovať nové trendy a prispôsobovať sa novým hrozbám a technológiám.

Odborník na kybernetickú bezpečnosť musí mať široký súbor technických, analytických a komunikačných zručností, ktoré mu umožňujú identifikovať, analyzovať a riešiť rôzne hrozby a zraniteľnosti v digitálnom prostredí a vedieť im zabrániť a do budúcnosti predchádzať.

Študijný odbor tak predpokladá prirodzený záujem uchádzačov o:

- bezpečnostný aspekt v oblasti počítačových sietí
- oblasti architektúry IT riešení
- systémové a aplikačné softwarové riešenia
- programovanie
- oblasť databázových systémov
- IT e-služieb ako šifrovanie, využitie certifikátov, antivírové služby, firewaly

Predpokladom budúcej uplatniteľnosti absolventa je mať okrem technických, analytických a manažérskych zručností aj schopnosť komunikovať bezpečnostné riziká aj v kritických situáciách. V neposlednom rade by mal mať pevné etické zásady, ktoré sú nevyhnutné pri práci s citlivými informáciami a v rámci ochrany organizácie pred kybernetickými hrozbami. Musí byť pripravený na to, že sa od neho bude vyžadovať neustále učenie sa a prispôsobovanie sa novým technológiám a hrozbám.

Ide o špecializovaný a technicky náročný odbor, ktorý vyžaduje rôzne osobnostné a odborné predpoklady. Cieľové skupiny žiakov základných škôl pre oblasť štúdia kybernetickej bezpečnosti môžu byť:

- Žiaci so záujmom o IT – majú prirodzený záujem o počítače, technológie, internet a nové technologické trendy. Môže sa to prejaviť hraním hier, programovaním, experimentovaním s počítačmi, alebo záujmom o spôsob fungovania počítača.
- Žiaci so záujmom o programovanie a počítačové siete.
- Žiaci so záujmom o matematiku so silnými analytickými schopnosťami a schopnosťami riešiť problémy.
- Žiaci, ktorí sú zvedaví a zaujímajú sa o to, ako veci fungujú.
- Žiaci, ktorí sú ochotní neustále sa učiť a prispôsobovať sa novým výzvam.
- Žiaci, ktorí sú jazykovo zdatní a nerobí im problém študovať cudzojazyčnú literatúru.
- Žiaci, ktorí sú schopní pracovať v tíme a pracovať pod stresom.
- Žiaci, ktorí majú zmysel pre etiku a dodržiavanie zákonov a spoločenských noriem.

Môžu to byť žiaci, ktorí sa zapájajú do rôznych súťaží a predmetových olympiád, ale aj silno introvertní žiaci, ktorí sa navonok neprejavujú.

Cieľové skupiny rodičov žiakov základných škôl pre oblasť štúdia kybernetickej bezpečnosti môžu byť:

- Rodičia, ktorí sú technologicky zdatní a chcú, aby sa ich deti vzdelávali vo vysoko perspektívnej oblasti.
- Rodičia, ktorí veria, že budúcnosť patrí technológiám a chcú zabezpečiť perspektívu svojim deťom.
- Rodičia, ktorí chcú zabezpečiť svojim deťom finančne zaujímavú prácu.
- Rodičia, ktorí pracujú v oblasti IT príp. kybernetickej bezpečnosti a vidia toto uplatnenie ako vhodné aj pre svoje deti.
- Rodičia, ktorí si uvedomujú výhody štúdia tohto odboru – široké možnosti uplatnenia, takmer nulová hrozba nezamestnanosti, možná výhoda – práca z domu.
- Rodičia, ktorí vnímajú prácu v oblasti kybernetickej bezpečnosti ako atraktívnu, perspektívnu a prínosnú pre spoločnosť.

Možná perspektíva uplatnenia absolventov

Znalostné štandardy definované vo vyhláške, ktorou sa ustanovujú znalostné štandardy v oblasti kybernetickej bezpečnosti, tvoria rámec pre vytvorenie vzdelávacích programov na vzdelávacích inštitúciách, čím sa vypĺňa priestor nielen pre budovanie kvalitného bezpečnostného povedomia v oblasti kybernetickej bezpečnosti, ale aj pre zvyšovanie kvality vzdelávacích procesov, čo má tendenciu ovplyvniť následne aj kvalitu pracovníkov vykonávajúcich činnosti v oblasti kybernetickej bezpečnosti ako v štátnych tak aj v súkromných organizáciách.

Predmetná vyhláška okrem povinných rolí manažéra a audítora KB a už spomínaného špecialistu kybernetickej bezpečnosti ustanovuje nasledujúce roly v kybernetickej bezpečnosti:

- **tester kybernetickej bezpečnosti** – zodpovedný za testovanie zmien v prostrediach sietí a informačných systémov z pohľadu kybernetickej bezpečnosti,
- **architekt kybernetickej bezpečnosti** – zodpovedný za navrhovanie informačnej architektúry a bezpečnostných opatrení v oblasti kybernetickej bezpečnosti,
- **špecialista riadenia rizík** – zodpovedný za analýzu a riadenie rizík v oblasti kybernetickej bezpečnosti a ochrany údajov,

- **špecialista pre analýzu digitálnych stôp** – zodpovedný za vyhľadávanie a forenzné analýzy stôp v kybernetickom priestore,
- **špecialista pre riadenie súladu** – zodpovedný za to, že všetky smernice, politiky, riadiace aj prevádzkové procesy a postupy v organizácii sú v súlade s platnou právnou úpravou v oblasti kybernetickej bezpečnosti, ako aj s požiadavkami ostatných všeobecne záväzných právnych predpisov a noriem,
- **špecialista pre riešenie kybernetických incidentov** – zodpovedný za zachytávanie, analýzu a riešenie bezpečnostných udalostí,
- **výskumník** – zodpovedný za vyhľadávanie zraniteľností systémov, identifikáciu príčin zraniteľností a hrozieb, overovanie zdrojového kódu, testovanie odolnosti systémov, identifikáciu chýb bezpečnostných mechanizmov a vyhodnocovanie efektivity bezpečnostných opatrení,
- **lektor** – zodpovedný za realizáciu vzdelávacích aktivít v oblasti kybernetickej bezpečnosti a ochrany údajov.

Znalostné štandardy definujú požiadavky na vedomosti, zručnosti, kompetencie, odbornú prax a stupeň vzdelania. Niektoré z definovaných rolí (napr. architekt kybernetickej bezpečnosti či špecialista pre riadenie súladu) môžu zastávať zamestnanci s ukončeným úplným stredným všeobecným alebo úplným stredným odborným vzdelaním s požadovanou odbornou praxou v oblasti.

Vytvorenie príslušných študijných odborov, resp. inovovanie už existujúcich odborov by však bolo vhodným predpokladom získania kvalifikovanej odbornej pracovnej sily aj na ďalšie bezpečnostné role, ktoré si nevyžadujú vysokoškolské vzdelanie.

Z uvedeného vyplýva, že absolvent študijného odboru má perspektívu uplatnenia v oblasti kybernetickej bezpečnosti, ale aj v ďalšom vzdelávaní a tým aj v kariérnom raste, pretože je to oblasť, ktorá má potenciál a jej význam sa bude v budúcnosť zvyšovať.

ZOZNAM POUŽITEJ LITERATÚRY

1 https://cybercompetence.sk/slovensko-potrebuje-odbornikov-na-kyberneticku-bezpecnost/

2 https://ec.europa.eu/regional_policy/en/policy/how/priorities

3 https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_sk,

4 https://digital-strategy.ec.europa.eu/en/activities/digital-programme

5 https://www.edihnetwork.eu/home

6 https://digital-strategy.ec.europa.eu/en/activities/cef-digital

7 https://www.mirri.gov.sk/wp-content/uploads/2019/06/Strategia-digitalnej-transformacie-Slovenska-2030.pdf

8 https://mirri.gov.sk/sekcie/informatizacia/digitalna-transformacia/akcny-plan-digitalnej-transformacie-slovenska-na-roky-2023-2026/

9 https://education.ec.europa.eu/focus-topics/digital-education/action-plan

10 https://www.minedu.sk/data/att/23246.pdf

11 https://www.minedu.sk/data/att/23247.pdf

12 https://rokovania.gov.sk/RVL/Material/27932/1

13 https://rokovania.gov.sk/RVL/Material/27931/1

14 https://www.mirri.gov.sk/wp-content/uploads/2022/01/Strategia-DESI-do-roku-2025.pdf

15 https://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=CELEX:52020JC0018

16 https://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=CELEX:32022L2555

17 https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2018/69/

18 https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2022/492/

19 https://www.nbu.gov.sk/narodna-strategia-kybernetickej-bezpecnosti-na-roky-2021-az-2025/

20 https://www.nbu.gov.sk/akcny-plan-kybernetickej-bezpecnosti/

21 https://cybercompetence.sk/slovensko-potrebuje-odbornikov-na-kyberneticku-bezpecnost/

22 https://www.kvalifikacie.sk/karta-kvalifikacie/1387

23 https://www.sustavapovolani.sk/register-zamestnani/pracovna-oblast/karta-zamestnania/17928-specialista-kybernetickej-bezpecnosti/

24 https://www.nbu.gov.sk/certifikacia-manazera-kybernetickej-bezpecnosti/

25 https://www.planobnovy.sk/kompletny-plan-obnovy/efektivna-verejna-sprava-a-digitalizacia/

26 https://eurofondy.gov.sk/program-slovensko/

27 https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:32021R0887&from=SK

28 https://mirri.gov.sk/plan-obnovy/vyzvy/zverejnenie-vyzvy-na-predkladanie-ziadosti-o-poskytnutie-prostriedkov-mechanizmu-na-vytvorenie-kompetencnych-centier-kybernetickej-bezpecnosti/

29 https://ucv.uniza.sk/vzdelavanie-zamestnancov-uniza/inovacne-vzdelavanie/

30 https://www.nbu.gov.sk/prevadzkovatelia-zakladnej-sluzby/

Republiková únia zamestnávateľov, Digital Park III, Einsteinova 19, 851 01 Bratislava 5
tel.: +421-2-3301 4280, ruz@ruzsr.sk, www.zamestnavatelia.sk