MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY

ŠTÁTNY INŠTITÚT ODBORNÉHO VZDELÁVANIA

DODATOK č. 6

ktorým sa mení
ŠTÁTNY VZDELÁVACÍ PROGRAM
pre odborné vzdelávanie a prípravu, skupinu študijných odborov

25 INFORMAČNÉ A KOMUNIKAČNÉ TECHNOLÓGIE

Schválený Ministerstvom školstva, vedy, výskumu a športu Slovenskej republiky dňa 5. októbra 2016 pod číslom 2016-9967/41446:31-10E0
s účinnosťou od 1. septembra 2017 začínajúc prvým ročníkom.

SCHVÁLILO

Ministerstvo školstva, vedy, výskumu a športu Slovenskej republiky dňa 10. júla 2023 pod číslom 2023/5272:60-C2910 s účinnosťou od 1. septembra 2023 začínajúc prvým ročníkom.

1 ÚVOD DO ŠTÁTNEHO VZDELÁVACIEHO PROGRAMU

1.3 Záznamy o platnosti a revidovaní štátneho vzdelávacieho programu

Štátny vzdelávací program vyššieho odborného vzdelania

Platnosť ŠVP Dátum	Revidovanie ŠVP Dátum	Záznam o inovácii, zmenách úpravách a pod.
01. 09. 2023	**apríl 2023**	**Zmena:** 1. Doplnenie študijného odboru „špecialista informačnej bezpečnosti; špecialistka informačnej bezpečnosti“, za študijný odbor „počítačové systémy“ na s. 14 v kapitole 4 Osobitosti a podmienky vzdelávania žiakov so špeciálnymi výchovno-vzdelávacími potrebami. 2. Vloženie vzdelávacích štandardov študijného odboru „špecialista informačnej bezpečnosti; špecialistka informačnej bezpečnosti“ za vzdelávacie štandardy študijného odboru „počítačové systémy“ na s. 63. **Odôvodnenie:** Doplnenie obsahu štátneho vzdelávacieho programu v nadväznosti na úspešné ukončenie experimentálneho overovania študijného odboru „špecialista informačnej bezpečnosti; špecialistka informačnej bezpečnosti“ k 31. 08. 2023.

1. **Na s. 14 v časti 4 Osobitosti vzdelávania žiakov so špeciálnymi výchovno-vzdelávacími potrebami, vyššie odborné vzdelanie** sa pod slová „počítačové systémy“ vkladá slovo „špecialista informačnej bezpečnosti; špecialistka informačnej bezpečnosti“.

2. V kapitole **16 Vzdelávacie oblasti a podkapitole Vzdelávacie štandardy spoločné pre všetky študijné odbory** sa na s. 63 za vzdelávacie štandardy za študijný odbor „počítačové systémy“ vkladajú vzdelávacie štandardy pre študijný odbor „špecialista informačnej bezpečnosti; špecialistka informačnej bezpečnosti“, ktoré znejú:

„

Študijný odbor ***ŠPECIALISTA INFORMAČNEJ BEZPEČNOSTI*** ***ŠPECIALISTKA INFORMAČNEJ BEZPEČNOSTI***
TEORETICKÉ VZDELÁVANIE
Výkonové štandardy
Absolvent má: - efektívne a plynule používať osvojené jazykové prostriedky, - komunikovať v rôznych, bežných aj špecifických situáciách a spoločenských úlohách a preukázať osvojené jazykové prostriedky a komunikatívne kompetencie v rodnom aj cudzom jazyku, - uviesť a aplikovať základné zásady a pravidlá spoločenského styku, - vhodne vybrať, popísať a aplikovať formy a techniky verbálnej komunikácie a neverbálne jazykové prostriedky,

- definovať zásady BOZP, PO a hygieny pri práci, charakterizovať bezpečnostné normy a štandardy zákazníka a spoločnosti,
- popísať TCP/IP protokoly a bezpečnostné koncepty a zariadenia, ako je firewall, inšpekcie aplikačnej vrsty (IPS, Proxy), demilitarizovaná zóna (DMZ), Virtuálna Privátna sieť (VPN), šifrovanie, úpravy sieťovej prevádzky NAT a PAT, kontrolné metódy a zoznamy riadenia prístupu (Access Control List ACL, AAA, 802.1x, Radius, Tacacs+, NAC),
- uviesť možné útoky v sieťovom prostredí a možnosti obrany voči nim (napr. DoS, DDoS, a pod.),
- popísať a vysvetliť základné techniky programovania aspoň v jednom vyššom programovacom a/alebo skriptovacom jazyku (Java, C++, Python, PHP a pod.),
- definovať sieťovú bezpečnostnú architektúru,
- definovať princíp symetrického a asymetrického šifrovania, definovať zásady auditorských postupov,
- vytvoriť návrh riešenia zabezpečenia siete na základe modelovej situácie,
- identifikovať a vyhodnocovať bezpečnostné riziká, hrozby a prieniky,
- monitorovať dodržiavanie a vykonávanie skúšky kontroly kvality výstupov voči bezpečnostným požiadavkám,
- vykonávať pravidelné kontroly bezpečnostných procesov, ako je stabilita siete,
- kontrolovať aplikované bezpečnostné filtre a skenovanie,
- vykonávať opatrenia na odstránenie bezpečnostných rizík, hrozieb, prieniku,
- implementovať platnú legislatívu ohľadom kybernetickej bezpečnosti pri tvorbe bezpečnostnej politiky,
- ovládať terminológiu a základné pracovné postupy pre prácu, správu, návrh a odstraňovanie porúch v IKT systémoch (najmä na úrovni infraštruktúry, vrátane operačných systémov, databázových systémov a pod.),
- popísať účel a formu zhromažďovania systémových a bezpečnostných hlásení v IKT systémoch a ich využitie pre riešenie poruchových stavov IKT systémov,
- ovládať terminológiu a základné pracovné postupy procesného a projektového riadenia moderných IKT riešení,
- popísať a vysvetliť koncept virtualizácie IKT prvkov a základnú terminológiu v tejto oblasti (VLAN, virtualmachine, hypervisor a pod.),
- analyzovať požiadavky zákazníka a navrhnúť jednoduché bezpečnostné riešenie.

Obsahové štandardy

Odborná jazyková príprava v cudzom jazyku

Počúvanie s porozumením – rozvoj sluchových spôsobilostí, počúvanie s porozumením monologických a dialogických prejavov, cudzojazyčných pokynov, inštrukcií a súvislých prejavov, ktoré obsahujú známe lexikálne a gramatické javy.

Čítanie s porozumením – rozvoj schopností čítať výrazne, so správnym prízvukom, intonáciou a melódiou, získavanie potrebných informácií z autentických cudzojazyčných materiálov, hľadanie kľúčových informácií v texte, pochopenie obsahovej podstaty textov, všeobecného, odborného a populárno-náučného charakteru. Na základe kontextu vydedukovať význam neznámych výrazov, využívať ilustrácie, tabuľky, schémy, používať slovníky, jazykové a iné príručky, používať rôzne jazykové prostriedky, ktoré skvalitnia výslovnosť a obohatia slovnú zásobu.

Písomný prejav – vyjadrovať sa k všeobecným i odborným témam, získať a poskytovať informácie v osobnej, verejnej a pracovnej oblasti, zrozumiteľne, v súlade s pravopisnými normami a štylisticky vhodne zaznamenať podstatné informácie z vypočutého, vyjadriť myšlienky, postoje, názory, opísať osoby, predmety a udalosti, zostaviť osnovu prečítaného (vypočutého) textu a reprodukovať obsah, vyplniť dotazník, tlačivá, žiadosti, zostaviť životopis, zostaviť a odpovedať na základný typ listu obchodnej korešpondencie, využívať slovníky, gramatické príručky.

Ústny prejav – jazykovo správne, zrozumiteľne a primerane situácii reagovať v bežných životných situáciách. Začať, rozvíjať a ukončiť rozhovor, predstaviť sa a predstaviť inú osobu, niekoho osloviť, pozdraviť, zablahoželať, o niečo požiadať, poďakovať, ospravedlniť sa a rozlúčiť sa, vyjadriť súhlas, odmietnutie, záujem a nezáujem radosť, sklamanie, pochybnosť, prekvapenie, ochotu, riešiť štandardné situácie, odpovedať na otázky a tvoriť otázky k prečítanému alebo vypočutému textu, vyjadriť hlavnú myšlienku textu a svoj postoj k prečítanému alebo vypočutému, vyjadriť svoj názor na určitý problém, opísať predmet, osobu, udalosť, miesto, charakterizovať vlastnosti niekoho, informovať o reáliách Slovenska a krajín študovaného jazyka.

Poznatky o krajinách študovaného jazyka – rozvoj a upevňovanie vedomostí všeobecného a odborného charakteru z krajiny príslušnej jazykovej oblasti, jej kultúry, tradícií a spoločenských udalostí.

Odborná konverzácia – rozvoj spôsobilosti žiaka efektívne používať cudzí jazyk v kontexte IKT, dôraz na schopnosť aplikovať špecifické vyjadrovacie prostriedky v rámci IKT odborov. Práca v tíme, práca s informáciami, schopnosť tvorby a realizácie prezentácie a následnej diskusie na odbornú tému, spôsobilosť kultivovane komunikovať písomnou formou – emailom, správou, technickou dokumentáciou a pod.

Človek a spoločnosť, komunikácia

Osvojenie odbornej terminológie vied o človeku a spoločnosti na úrovni primeraného použitia vo verbálnej i neverbálnej komunikácii s odbornou i laickou verejnosťou. Základy edukačných, psychologických a sociologických vied. Poznanie klienta z hľadiska psychických procesov, stavov, štruktúry osobnosti, špecifík z hľadiska ontogenézy, sociálneho prostredia.

Využitie pri komunikácii so svojim okolím – zákazníkom či používateľom IKT riešenia, pochopenie potrieb a požiadaviek partnera v projekte či procese. Motivácia spolupracovníkov či podriadených.

Riadenie podnikov, procesov, projektov a služieb v IKT

Základné manažérske funkcie – plánovanie, organizovanie, vedenie a kontrola. Informácie pre rozhodovanie a efektívnu prácu riadiaceho pracovníka.

Riadenie ľudských zdrojov – základné zásady a pravidlá spoločenského styku, foriem a techník verbálnej komunikácie a neverbálnych jazykových prostriedkov. Používanie jazykových prostriedkov v rôznych, bežných aj špecifických situáciách a úlohách. Náročnosť profesie, osvojenie techník sebapoznania a hodnotenia vlastnej práce a práce iných, s dôrazom na rešpektovanie a dodržiavanie etických princípov. Špecifiká dodávky IKT produktov a služieb – služba a IT služba, proces a IKT proces, návrh a rozpoznanie kľúčovej charakteristiky efektívnej IKT služby – v kontexte jej outsourcingu. Schopnosť vytvoriť jednoduchý projekt, jednoduchý podnikateľský plán a SWOT analýzu silných a slabých stránok existujúcej či novej IKT služby, produktu, riešenia, a pod.

Budovanie právneho vedomia, súvisiace s výkonom riadiacich činností, využívanie platného právneho poriadku a ustanovení obchodného, občianskeho, živnostenského a pracovného práva. Právne aspekty informatiky - oboznámenie žiakov so základnými právnymi aspektmi tvorby softvéru. Obchodné spoločnosti, ich založenie, vznik a zánik obchodných spoločností, živnostenské podnikanie. Uzatváranie obchodných zmlúv, zabezpečenie obchodných záväzkov, zodpovednosti v obchodnom práve. Elektronické právne úkony, ako sú elektronický podpis a zaručený elektronický podpis, s prostriedkami realizácie elektronického podpisu, podpisovaním a overovaním elektronického podpisu. Elektronický obchod, právna úprava elektronického obchodu. Autorské právo a ochrana osobných údajov. Rešpektovanie intelektuálneho vlastníctva a autorstva informatických produktov, systémov a aplikácií.

Operačné systémy

Štruktúra, činnosť a použitie operačných systémov (OS) a jednotlivých modulov pre správu systémových prostriedkov. Stratégie použité pri správe systémových prostriedkov, spôsoby komunikácie OS s používateľom a zabezpečenie dát na úrovni súborového systému.

Praktická časť: Inštalácia a konfigurácia operačných systémov (napr. MS Windows či GNU/Linux) pracujúcich ako pracovné stanice v homogénnych a heterogénnych sieťach, servery a serverové klastre. Vedomosti, zručnosti a praktické skúsenosti z oblasti nasadenia OS v sieťovom prostredí.

Konfigurácia hardvérových nastavení, bootovanie systému, vrstvený návrh HDD, inštalácia boot manažéra, manažovanie zdieľaných knižníc. Verzia Debian „balíkový manažment“, RPM a YUM „balíkový manažment“ a práca s CLI, základný súborový manažment, procesy, textové súbory, Linuxové súborové systémy, vlastníctvo súborov a oprávnení.

Bezpečnosť počítačových sietí

Základný prehľad z oblasti moderných bezpečnostných systémov. Problematika bezpečnostných hrozieb v sieťach, koncept vírusov, červov, trójskych koňov, spyware a adware, útoky nultého dňa, odpočúvanie a krádež dát, spoofing a krádež identity. Zložky sieťového bezpečnostného systému (antivírusmi, bezpečnostnými bránami (firewallmi), systémy detekcie prieniku, VPN, atď.) Kryptografia a kyberkriminalita, sledovanie možných sieťových útokov a navrhovanie bezpečnostných opatrení na zabránenie možných útokov.

Bezpečnosť databázových systémov

Teoretické základy v oblasti databázových systémov. Návrh databázy na základe požiadaviek a potrieb, vytvorenie databázy a implementácia databázy ako súčasť informačného systému. Zabezpečenie databázy a dát na niekoľkých úrovniach a spôsobmi, ktoré sú bežne dostupné. Základné princípy bezpečnosti sa zameriavajú na bezpečnostné politiky, analýzu rizík, riadenie prístupu v RDBMS, šifrovanie dát v DBMS, koncept CIA a bezpečnostné štandardy. Bezpečnostné modely obsahujúce informácie

o prístupe k databáze, typických bezpečnostných zraniteľnostiach a nedostatkoch, typických cielených útokoch na databázy, hrozbách a bezpečnostných opatreniach.

Základy kryptológie

Teoretické základy z oblasti kryptografie a počítačovej bezpečnosti. Analýza a návrh bezpečnostných riešení pre informačné a komunikačné systémy. Princípy používaných algebraických štruktúr, základných kryptografických pojmov (hashe, generátory náhodných čísel, základných algoritmov), fungovanie symetrických a asymetrických kryptosystémov. Kryptografia v základnom kontexte, kryptografia s tajným kľúčom, hašovacie funkcie, autentizačné kódy, problémy s asymetrickou kryptografiou, kryptografia s verejným kľúčom, hybridný systém: kombinácia symetrického a asymetrického šifrovania, digitálny podpis, distribúcia kľúčov, heslá, kyberkriminalita a kryptografické protokoly.

Bezpečnosť informačných systémov

Ochrana IS ako komplexu organizačných, programových, technických a sociálno-personálnych opatrení spojených s minimalizáciou možných strát vzniknutých v dôsledku poškodenia, zničenia alebo zneužitia IS. Zodpovednosť a riadenie prístupu, útokov a monitorovanie, ISO modelov, protokolov, sieťovej bezpečnosti a sieťovej infraštruktúre, bezpečnej komunikácii a protiopatreniach, konceptoch a princípoch bezpečnostného manažmentu, bezpečnostných politikách a rolách, zabezpečení dát a aplikácií, nežiadúcich kódoch a aplikačných útokoch, kryptografii a algoritmoch šifrovania symetrickým kľúčom, PKI a kryptografických aplikáciách. Princípy dizajnu PC, princípy bezpečnostných modelov, bezpečnostný audit a monitoring, plán zotavenia sa po útoku, základy práva a vyšetrovania, incidenty a etika, fyzické bezpečnostné požiadavky.

Programovanie

Základy algoritmizácie úloh, základné pojmy v oblasti programovania, algoritmické štruktúry, verzovacie systémy, ktoré tvoria neoddeliteľnú súčasť pri tvorbe komplexných aplikácií. Základné návrhové vzory, používané pri tvorbe aplikácií. Tvorba komplexnejších aplikácií s využitím databázových strojov, sieťových serverov, použitím zariadení IoT (Internet of Things) a vyhodnocovanie dát nameraných danými zariadeniami. Agilné metodológie pri tvorbe projektu.

PRAKTICKÁ PRÍPRAVA

Výkonové štandardy

Absolvent vie:

- popísať a vysvetliť základné koncepty vytvárania sietí a ich bezpečnosti (dráha/route, sieť, nslookup a pod.) a sieťových komponentov (smerovač, firewall, LAN, WAN, port a pod.),
- charakterizovať a vysvetliť účel komunikačných protokolov používaných pre IKT systémy (najmä TCP/IP, UDP a pod.),
- zapojiť prostriedky IKT systémov do rôznych typov sietí a správne nastaviť parametre takejto počítačovej siete,
- monitorovať a optimalizovať sieťový prenos v jednoduchom IKT prostredí kancelárie či menšej firmy,
- diagnostikovať prevádzkyschopnosť a funkčnosť počítačových sietí,
- vysvetliť spôsoby vzájomnej komunikácie jednotlivých častí a celkov informačných, serverových a sieťových technológií,
- orientovať sa v globálnych informačných sieťach,
- hodnotiť požadované návrhy a zmeny voči bezpečnostným normám,
- vytvárať vyhovujúce konfigurácie pre produkčné použitie,
- identifikovať a vyhodnocovať bezpečnostné riziká, hrozby a prieniky,
- vykonávať opatrenia na odstránenie bezpečnostných rizík, hrozieb, prieniku,
- kontrolovať aplikované bezpečnostné filtre a skenovanie,
- vykonávať pravidelné kontroly bezpečnostných procesov, ako je stabilita siete,
- monitorovať dodržiavanie a vykonávanie skúšky kontroly kvality výstupov voči bezpečnostným požiadavkám,
- používať metódy šifrovania pri zabezpečení informačného systému,
- pracovať pri riešení problémových úloh - projektu v tíme,
- vedieť implementovať SCRUM metodiku práce pri práci na projekte,
- vedieť prezentovať a obhájiť výsledok riešenia problémovej úlohy - projektu,
- vedieť si rozdeliť zodpovednosť za čiastkové úlohy pri tímovej spolupráci,
- riešiť jednoduché problémy integrácie IKT z praxe a zvoliť s ohľadom na technické a ekonomické požiadavky správne postupy riešenia,
- navrhnúť a previesť do počítačového kódu jednoduché softvérové aplikácie s využitím programovacieho či skriptovacieho jazyka vyššej úrovne,

- používať základné príkazy pre prácu s databázami, výber, vkladanie a úpravu údajov v databáze,
- vykonávať základné pracovné postupy pri algoritmickom návrhu, implementácii, testovaní a nasadení nových softvérových prostriedkov v IKT prostredí,
- vytvárať a interpretovať algoritmy pre jednoduché problémy.

Obsahové štandardy

Bezpečnosť počítačových sietí

Praktická príprava v oblasti bezpečnosti počítačových sietí- zabezpečenie prístupu k zariadeniam, priradenie administratívnych rolí, monitorovanie a riadenie zariadení, použitie automatizovaných bezpečnostných prvkov. Konfigurácia technológií Firewall, technológie IPS a VPN. Zabezpečenie LAN siete (ochrana pred útokmi na MAC tabuľku, VLAN útokmi, útokmi na protokol DHCP, ARP a STP).

Bezpečnosť databázových systémov

Implementácia bezpečnostných modelov zameraná na ochranu proti SQL injection, správu prístupov užívateľov, správa užívateľských oprávnení, riadenie prístupu k dátam, auditovanie a monitorovanie databázy, vysokú dostupnosť a ochrana pred stratou dát, maskovanie dát a ostatné bezpečnostné hľadiská.

Získavanie praktických zručností, samostatná práca žiakov s dôrazom na komunikáciu v skupine. Aktívna spolupráca žiaka na rozvoji vlastného poznania, ďalšieho sebavzdelávania, inovácie svojich vedomostí v dynamicky rozvíjajúcej sa oblasti.

Bezpečnosť informačných systémov

Zručnosti v oblasti bezpečnostného auditu a monitoringu - nástroje a techniky pre monitoring, spôsoby penetračného testovania informačného systému, nejasné hrozby a následné protiopatrenia. Zostavenie plánu zotavenia po útoku - stratégia zotavenia sa informačného systému, tvorba plánu zotavenia informačného systému, testovanie a údržba plánu zotavenia sa informačného systému.

Programovanie

Návrh počítačových programov, podrobná analýza úlohy, návrh riešenia, výber vhodných postupov a prvkov. Algoritmizácia úloh, využívanie štruktúrovaného programovacieho jazyka nariešenie úloh konzolového typu, ucelenosť a kompaktnosť algoritmov. Tvorba programov pre graficky orientovaný operačný systém s vysvetlením základov objektového programovania. Programovanie aplikácií pre jednoúčelové zariadenia, priama komunikácia s hardvérom, spracovanie vstupných signálov rôzneho druhu, rôzne spôsoby ovládania výstupov a medziprocesorová komunikácia. Pokročilé algoritmické techniky konzolových a grafických aplikácií, základy programovania verzovacích systémov a jazyka UML.

“.