VŠB TECHNICKÁ UNIVERZITA OSTRAVA | FAKULTA ELEKTROTECHNIKY A INFORMATIKY | KATEDRA TELEKOMUNIKAČNÍ TECHNIKY

OKRUHY STÁTNÍCH ZÁVĚREČNÝCH ZKOUŠEK

V **NAVAZUJÍCÍM MAGISTERSKÉM** STUDIJNÍM PROGRAMU**:**

KOMUNIKAČNÍ A INFORMAČNÍ TECHNOLOGIE

Předměty státní závěrečné zkoušky v akademickém roce 2023/2024:

I. **Komunikační a informační technologie** (2 otázky)

II. **Dle zvoleného zaměření** (2 otázky)

A. Zaměření: **KOMUNIKAČNÍ SÍTĚ**

B. Zaměření: **OPTICKÉ KOMUNIKACE A SENZORY**

C. Zaměření: **MOBILNÍ A RÁDIOVÉ KOMUNIKACE**

Datum: 14.2.2024
Autor: Ing. Zdeňka Chmelíková, Ph.D.
Kontakt: zdenka.chmelikova@vsb.cz

I. KOMUNIKAČNÍ A INFORMAČNÍ TECHNOLOGIE

Kybernetická bezpečnost I

a) Základy kryptografických systémů – pojmy Steganografie, Kryptologie, Kryptografie, Kryptoanalýza, principy moderní kryptografie – Kerckhoffsův princip.
b) b. Moderní kryptografie – Blokové vs. Proudové šifry, generátory náhodných čísel, módy blokových šifer.
c) c. Moderní kryptografie – Symetrická vs. Asymetrická kryptografie, Hashovací funkce, digitální podpis.
d) d. Principy PKI – tvorba certifikátu, význam, centralizovaný vs. Decentralizovaný model ověřování.
e) e. Rodina protokolů SSL/TLS – význam, výměna zpráv, využití v praxi, rozdíly mezi verzemi, cipher suits.
f) f. Zabezpečená vzdálená správa – protokoly SSH a RDP, principy zabezpečení, využití, výměna zpráv.
g) g. Virtuální privátní sítě – rodina protokolů IPsec, využití na vrstvách ISO/OSI, tunelový vs. transportní mód, praktické implementace VPN.
h) h. Monitoring a síťová analýza – důvody monitoringu a skenování poč. sítí, možnosti rozdělení dle protokolů, přístupu k síti – aktivní vs. pasivní monitoring, metriky pro monitoring.
i) Zabezpečení bezdrátových sítí – Wifi, Bluetooth, IoT, mobilní buňkové sítě – 4G a 5G.

Zpracování signálů v komunikacích II

a) Pojmy signál a soustava; rozdělení signálů. Pojmy frekvence a spektrum signálu.
b) Spektrum analogových a diskrétních signálů – Fourierovy řady, Fourierova transformace, diskrétní Fourierova transformace, FFT, diskrétní kosinusová transformace a jejich vlastnosti. Spektra základních typů signálů (jednotkový impulz, harmonický signál, obdélníkový signál).
c) Typický DSP systém (vzorkování, kvantování, kódování a rekonstrukce signálů); vzorkovací teorém, aliasing, leakage; kvantizační šum a jeho SNR.
d) Korelace 2 signálů a její význam, autokorelace a její význam. Konvoluce a její souvislost s LTI systémy. Souvislost korelace a konvoluce s Fourierovou transformací.
e) Linearita, stabilita, časová invariance, kauzalita soustav. Ideální a reálný filtr.
f) Filtry typu IIR a FIR. Jejich typické vlastnosti a oblasti použití, srovnání IIR a FIR.

Mobilní sítě

a) Buňkový princip, šíření elektromagnetických vln v mobilních buňkových sítích.
b) Systém LTE/SAE (kmitočtová pásma, architektura systému).
c) Systém LTE/SAE (OFDM a jednotka PRB, Cyclic Prefix, LTE Advanced).
d) Systém 5G NR (kmitočtová pásma, architektura systému).
e) Systém 5G NR (škálovatelný OFDM, CORESET, 5G Advanced).

f) Technologie a výstavba základnové stanice (části základnové stanice, hygienické limity, legislativa, optimalizace).

Měření v telekomunikační technice

a) Moderní koncept měřicího systému postavený na bázi virtuální instrumentace. Princip, výhody, HW a SW nástroje.
b) Měření, cíl měření, úplný výsledek měření, nejistota měření.
c) Vývojové prostředí LabVIEW pro návrh a realizaci SW části měřicího systému – popis, výhody.
d) Zdroje stimulačních signálů, osciloskopy, frekvenční analyzátory.
e) Analýza digitálně modulovaného signálu na fyzické vrstvě – konstelační diagram, prostředky používané pro jeho získání.
f) Vektor signálové generátory a vektor signálové analyzátory.

Praktikum komunikačních sítí II

a) Monitorování a správa komunikačních sítí (logování dat, NTP protokol, SNMP protokol, RRDtool pro tvorbu grafů, Netflow protokol).
b) Generování a sledování provozu v IP sítích (paketové generátory, hping, scapy, sledování provozu, wireshark, tcpdump, scapy).
c) Problematika AAA – autentizace, autorizace a účtování v komunikačních sítích (LDAP protokol, Radius, Kerberos, SSO systémy jednotného přihlášení, SAML).
d) Nástroje pro komunikaci (IRC komunikace, IM Instant Messaging, XMPP protokol, WebRTC komunikace pouze s prohlížečem).
e) Virtualizace – lxc/lxd kontejnery, možnosti zálohování.
f) Síťová automatizace, formáty dat, protokoly NETCONF, RESTCONF, WebAPI, Ansible.
g) Identity management, způsoby ověřování, více faktorové autentizační systémy.

Zaměření: Komunikační sítě

Pokročilé síťové technologie I

a) Technologie MPLS – základní vlastnosti (label, LSP, LDP, LIB, LFIB).
b) MPLS VPN, MPLS – Traffic Engineering, AToM, VPLS (VRF, VPNv4, RT, tunnel label a virtual circuit label).
c) Differentiated Services, způsoby označení priority přenášených dat (DSCP, IP precedence, ToS, CoS, Assured Forwarding).
d) Metody obsluhy paketových front (CBWFQ, LLQ), Traffic Shaping, Traffic Policing, WRED.

Tvorba multimediálního obsahu

a) Kompozice záběru (typy záběrů – velikost, pohyb, zlatý řez), Snímková frekvence, prokládaní obrazu, rozlišení a poměr stran
b) Osvětlení, vyvážení bílé
c) NLE – nelineární střižny, klíčování
d) Produkce, postprodukce, streamování
e) Režijní pracoviště

Pokročilé síťové technologie II

a) Softwarově definované sítě – koncepce, varianty (Open SDN, API SDN, Overlay SDN), srovnání s tradičními sítěmi a typické příklady využití.
b) Protokoly a jazyky v softwarově definovaných sítích (OpenFlow, P4, EVPN, VXLAN, atp.), jejich vlastnosti a srovnání.

Kybernetická bezpečnost II

a) AAA – principy, protokoly, autentizační schémata, RADIUS vs. Diameter, SSO
b) b. Firewally – rozdělení, funkce, Netfilter – nástroje iptables a nft, příklady tabulek, řetězců a vytváření pravidel.
c) Biometrická autentizace – identifikace a verifikace, biometrický systém, používané biometrické metody a jejich srovnání, identifikace řečníka.
d) d. Penetrační a výkonové testování – principy bezpečnostního a výkonového testování, systémy pro penetrační testy, metody bezpečnostního auditu.
e) e. Kvantová distribuce klíče – principy kvantové kryptografie a kvantové výměny klíčů, QKD protokoly, bezpečnost QKD a srovnání s klasickými metodami výměny klíčů.
f) f. Legislativa v komunikační bezpečnosti – národní a mezinárodní právo a legislativa v oblasti kybernetické bezpečnosti – NIS a NIS2, GDPR, Zákon o kybernetické bezpečnosti a Zákon o ochraně osobních údajů.

g) g. Systémy pro autonomní a bezpečnostní monitoring sítí – IDS a IPS systémy, principy funkce, nasazení v síti, detekce útoků, signatury, nástroj Suricata – pravidla a jejich tvorba,
h) h. Bezpečnost v multimédiích – zabezpečení služby VoIP – bezpečnost protokolů SIP, RTP, SRTP, SRTP-DTLS, rizika a útoky v IP telefonii.
i) Honeypoty a honeynety – použití v síti, princip funkce a typy, praktické nástroje a nejčastěji simulované služby.

Modelování a dimenzování sítí

a) Dimenzování a klasifikace obsluhových systémů.
b) Modely využívané pro simulaci ztrátovosti a zpoždění.
c) Discrete Event Simulation, definice QoS a QoE.

Virtualizace II

a) Srovnání virtuálních systémů a kontejnerů, hypervizory typu I a typu II, možnost škálování a nasazování.
b) Zálohování, obnova a replikace virtuálních systémů – popis, softwarové nástroje.
c) Zajištění vysoké dostupnosti u virtuálních systémů – replikace a možnosti použití, geo-replikace, RPO (Recovery Point Objective).
d) Nastavení a konfigurace sítí u nástrojů pro virtualizaci a kontejnerizaci – oddělení provozu, NAT, Bridge.
e) Snapshoty – popis, využití, výhody a nevýhody.
f) Kontejnery – popis, technologie, instalace a nastavení, možnost záloh a migrace, aplikační a systémové kontejnery.
g) Škálovatelnost u kontejnerů, nástroje pro správu kontejnerů, popis fungování těchto nástrojů.
h) Nástroje pro kontejnery – popis nástrojů, srovnání, typické využití, monitoring kontejnerů.
i) Komerční nástroje pro kontejnery – popis, vzájemné srovnání, srovnání s tzv. “self-hosted” řešením.

Zaměření: Optické komunikace a senzory

Optické komunikace I-III

a) Popis světla – paprskový, vlnový, kvantový. Pojmy parsek, vlnoplocha, foton. Energie fotonu. Fermatův princip, Snellův zákon lomu. Koherence, polarizace a interference světelného záření.
b) Popis světla – paprskový, vlnový, kvantový. Pojmy parsek, vlnoplocha, foton. Energie fotonu. Fermatův princip, Snellův zákon lomu. Koherence, polarizace a interference světelného záření.
c) Zdroje pro optické komunikace – LED, laser – fyzikální principy, společné vlastnosti a rozdíly. Spontánní a stimulovaná emise záření. Inverze populace, čerpání.
d) Detektory pro optické komunikace – fotodioda, PIN, lavinová fotodioda (APD) – fyzikální principy; vazba na parametry SNR a BER.
e) Měření útlumu na optických trasách. (Typy a druhy přímé metody a nepřímá metoda).
f) Speciální materiály a struktury optických vláken. Vlákna s posunutou disperzní charakteristikou. Vlákna necitlivá na ohyb. Braggovská vlákna. Mikrostrukturní vlákna.
g) Nelineární jevy v optických vláknech. Ramanův a Brillouinnův rozptyl. Čtyřvlnné směšování. Vlastní fázová modulace, solitony. Vzájemná fázová modulace.
h) Měření disperzních jevů v optických komunikacích. Druhy měřicích metod pro měření chromatické či polarizační vidové disperze.
i) WDM systémy – popis typů xWDM systémů, optické vláknové zesilovače pro optické sítě a polovodičové zesilovače, filtry, optické děliče – typy. Kompenzátory chromatické disperze.
j) Technologie výroby optických vláken a kabelů.
k) Spojování optických vláken – mechanické spojky, svařování, konektorování.
l) Vláknově optické senzory, dělení, využívané principy, bodové a distribuované senzory.

Vláknově optické senzory II

a) Rozdíly mezi komunikačními a senzorickými vlákny. Rozdělení vláknově optických senzorů dle prostorového rozložení měřené veličiny. Rozdělení vláknově optických senzorů dle způsobu modulace měřené veličiny, intrinzitní vs extrinzitní způsob snímání veličiny.
b) Fotoelektrický jev. Elektrooptický jev.
c) Modulátory optického záření – rozdělení. Blokové modulátory. Integrované optické modulátory.
d) Intenzitní senzory, principy činnosti.
e) Interferometrické senzory, Mach-Zehnderův interferometr, Michelsonův interferometr. Sagnacův interferometr.
f) Mřížkové optické senzory. Výroba mřížek. Fotosenzitivita.
g) Rayleighův, Ramanův a Brillouinův rozptyl. Princip DTS. Princip DSTS

Vláknově optické senzory III

a) Tepelné účinky laserového záření, Interakce světlo – pokožka, Barvy a jejich vliv na člověka
b) Optické vlákna, jejich základní vlastnosti a možnosti využití jako biosenzory
c) Intenzitní senzory: vlastnosti, princip funkce a jejich možnosti aplikace v biomedicíně.
d) Fázové senzory: vlastnosti, princip funkce a jejich možnosti aplikace v biomedicíně.
e) Spektroskopické senzory: vlastnosti, princip funkce a jejich možnosti aplikace v biomedicíně.
f) Speciální vláknově optické biosenzory: polymerní vlákna, tapering, mikrostrukturní vlákna, polarizační senzory, pH senzory apod.
g) Zpracování dat z optických a optovláknových senzorů: filtrace signálu, aplikace pokročilých metod zpracování.

Optické bezvláknové systémy

a) Základní koncept optické bezvláknové sítě, charakteristika přenosového média – atmosféry (atmosférické jevy, extinkce, scintilace), typy bezvláknových sítí, prvky bezvláknových sítí,
b) Používané typy linkových kódů a modulačních formátů pro komunikaci, komunikační systémy ve viditelném spektru.

Zaměření Mobilní a rádiové komunikace (0 studentů pro AR23/24)

1. **Mobilní komunikační zařízení**
2. **Tvorba aplikací mobilních zařízení II**
3. **Kybernetická bezpečnost II Operační systémy mobilních zařízení**
4. **Provozování rádiových sítí**
5. **Mobilní systémy**