

Informačný list predmetu

Akademický rok 2026/2027

Vysoká škola	Univerzita sv. Cyrila a Metoda v Trnave
Fakulta	FPV UCM
Kód predmetu	KAI/bd31/25
Názov predmetu	informačná bezpečnosť
Rozsah	2P + 2C
Počet kreditov	4
Vyučujúci	doc. RNDr. PaedDr. Ladislav Huraj, PhD. (prednášajúci)

Podmienky na absolvovanie predmetu

Študenti budú priebežne každý týždeň na seminároch prezentovať výsledky individuálneho štúdia, v skúšobnom období absolvujú záverečnú písomnú skúšku z predmetu.

Hodnotenie:

A 1,0 výborne – vynikajúce výsledky len s minimálnymi chybami < 92-100 % >

B 1,5 veľmi dobre – nadpriemerné výsledky s menšími chybami < 83-91 % >

C 2,0 dobre – vcelku dobré, priemerné výsledky < 74-82 % >

D 2,5 uspokojivo – dobré výsledky, ale vyskytujú sa významné chyby < 65-73 % >

E 3,0 dostatočne – výsledky vyhovujú minimálnym kritériám < 56-64 % >

FX* 4,0 nedostatočne – absolvovanie predmetu si vyžaduje vynaložiť ešte značné úsilie a množstvo práce zo strany študenta < 0-55 % >

Výsledky vzdelávania

Cieľom predmetu je

- porozumenie hrozieb, zraniteľnosti a výsledných rizík spojených s IKT, mechanizmov a opatrení na ich elimináciu alebo redukciu, ako aj predpokladov a dôsledkov ich realizácie,
- porozumenie podstaty bezpečnostných požiadaviek na IKT a možností ich naplnenia,
- schopnosť navrhnuť, realizovať, udržiavať a prevádzkovať mechanizmy na naplnenie bezpečnostných požiadaviek na IKT,
- schopnosť byť kvalifikovaným partnerom pre spoluprácu so špecialistami v IB.

Stručná osnova predmetu

Stručná osnova predmetu:

Prednášky

1. Manažment informačnej bezpečnosti.
2. Architektúra, modely a hodnotenie. Riadenie prístupu.
3. Aplikačná bezpečnosť.
4. Bezpečnosť prevádzky.
5. Kryptografia – základné pojmy.
6. Kryptografia symetrická – prúdové a blokové šifry, módy šifier.
7. Kryptografia asymetrická.
8. Digitálny podpis a jeho aplikácie.
9. Plánovanie kontinuity činností.

10. Biometrické systémy. Kľúčové hospodárstvo.

Seminár

1. Správa rizík, Klasifikácia údajov, Zodpovednosti a roly, Bezpečnostná politika, procedúry, štandardy, Organizačné zabezpečenie IB.
2. Architektúra IT prostredia organizácie, Bezpečnostné modely, Kritériá hodnotenia bezpečnosti počítačových systémov, Certifikácia systémov. Identifikácia, Autentizácia, Systémy pre riadenie prístupu, Politika riadenia prístupu, Manažment prístupu používateľov, Povinnosti používateľov, Záruky a uistenie, Ochrana prístupu k sieti.
3. Škodlivý kód, Aplikačná bezpečnosť.
4. Prevádzka hardvéru, Softvér, aplikácie, Dáta, Personálna bezpečnosť, Procesy.
5. Správa kryptografických kľúčov, Key escrow, PKI, Kryptografické protokoly, Kryptografické štandardy.
6. Digitálny podpis – PGP softvér, certifikačné authority, Registračná autorita pri UCM pre SlovakGrid CA SAV.
7. Technológie počítačových sietí, zraniteľnosti a riziká, Typy útokov na počítačové siete.
8. Plány a postupy obnovy činnosti, Dokumentácia a testovanie plánov.
9. Biometrické systémy – otlačok prsta, scan sietnice.
10. Legislatíva a etika - vyhlášok a štandardov SR v oblastiach: ochrana osobných údajov a súkromia, ochrana utajovaných skutočností. Certifikáty, certifikačná autorita, Web of Trust.

Odporúčaná literatúra

Kolouch, J. CyberSecurity, CZ.NIC, z.s.p.o. 2019

<https://web2.mlp.cz/koweb/00/04/49/72/14/cybersecurity.pdf>

Burda, K. Kryptografie okolo nás, CZ.NIC, z.s.p.o. 2019

https://knihy.nic.cz/media/filer_public/c8/84/c8847707-273e-4d03-b550-22f1ddcb7c1c/kryptografie_okolo_nas.pdf

Menezes, Alfred J., Paul C. Van Oorschot, and Scott A. Vanstone. Handbook of applied cryptography. CRC press, 2016. Dostupné na: <https://cacr.uwaterloo.ca/hac/>

Huraj, L., Šimon, M., Hrinkino, D.: Vybrané kapitoly zo sieťovej bezpečnosti: Základy a ich aplikácie. 1. vyd., Trnava: UCM. 2023, p. 145, ISBN: 978-80-572-0375-9.

Huraj, L., Šimon, M.: Cloudové a gridové technológie: princípy a bezpečnosť. 1. vyd., Banská Bystrica: Belianum. 2019, p. 153, ISBN: 978-80-557-1660-2.

Jazyk, ktorého znalosť je potrebná na absolvovanie predmetu

slovenský a anglický jazyk

Poznámky

profilový predmet