Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Návrh obsahu a harmonogramu postgraduálneho štúdia informačnej bezpečnosti

Bratislava, september 2014

KPMG
cutting through complexity™

1 Úvod

Postgraduálne štúdium informačnej bezpečnosti (IB) vychádza po obsahovej stránke zo špecifikácie MF SR, uvedenej v Zmluve medzi MF SR a KPMG Slovensko, s.r.o.,[1] spresnenej na základe požiadaviek účastníkov kurzov IB, organizovaných na základe tej istej zmluvy.

2 Obsah a rozsah štúdia

Postgraduálne štúdium obsahovo pokrýva nasledujúce oblasti[2]

Oblasť	**počet predná-šok**	**počet hodín**
1. Manažment	6	24
2. Bezpečnosť operačných systémov	5	20
3. Bezpečnosť počítačových sietí	7	28
4. Kryptológia	14	40
5. Právo	1	4
6. Elektronický podpis a PKI	2	8
7. Forenzná analýza	2	8
8. Riešenie bezpečnostných incidentov	1	4
9. Škodlivý softvér	2	8
spolu	40	144

3 Personálne zabezpečenie vzdelávania

Výučbu v PGŠ IB zabezpečujú

1. prof. RNDr. Otokar Grošek, CSc., FEI STU (kryptológia)
2. doc. RNDr. Daniel Olejár, PhD.,mimoriadny profesor, FMFI UK, (manažment IB, právo, PKI a elektronický podpis)

[1] Zmluva o poskytovaní služieb pri vypracovaní štandardov základných znalostí, metodických materiálov, analýz dokumentov a súvisiacich vykonávacích predpisov a realizácia školení pre oblasť informačnej bezpečnosti

[2] počty prednášok a hodín zodpovedajú obsahu prednášok, ale z organizačných dôvodov môžu byť prednášky zaradené do iného bloku

3. doc. Ing Ladislav Hudec, CSc., FIIT STU (manažment IB a bezpečnosť počítačových sietí)
4. doc. RNDr. Martin Stanek, PhD. FMFI UK, (kryptológia)
5. doc. RNDr. Karol Nemoga, PhD. SAV (kryptológia)
6. doc. Ing. Pavol Zajac, PhD. FEI STU (kryptológia)
7. doc. Ing. Milan Vojvoda, PhD., FEI STU (kryptológia)
8. RNDr. Jaroslav Janáček, PhD. FMFI UK, (bezpečnosť operačných systémov)
9. RNDr. Richard Ostertág, PhD., FMFI UK, (bezpečnosť operačných systémov a počítačových sietí)
10. RNDr. Michal Rjaško, PhD, FMFI UK, (kryptológia)
11. Mgr. Marek Sýs, PhD. FEI STU (kryptológia)
12. RNDr. Peter Košinár, ESET (škodlivý softvér)
13. Slavomír Ivančík, CSIRT.SK (bezpečnosť počítačových sietí)
14. Mgr. Lukáš Hlavička, CSIRT.SK (forenzná analýza)
15. Mgr. Martin Jurčík, CSIRT.SK (riešenie bezpečnostných incidentov)
16. Ing. Peter Jurík, CSIRT.SK (bezpečnosť počítačových sietí)
17. Ing. Michal Majerčík, CSIRT.SK (bezpečnosť počítačových sietí)
18. Ing. Marek Repka, FEI STU (kryptológia)

Richard Ostertág alternuje Jaroslava Janáčka a Martina Staneka a Michal Rjaško Martina Staneka.

Odbornými garantami štúdia su Daniel Olejár a Ladislav Hudec.

4 Organizácia štúdia

Štúdium je organizované v dvojdňových blokoch. Náplň blokov tvoria tematicky príbuzné prednášky, prípadne iné formy výučby. Keďže v ponuke PGŠ sú aj špecializované predmety v rozsahu menšom ako 16 hodín, zoskupili sme celú výučbu do troch väčších skupín:

Riadenie informačnej bezpečnosti (manažment IN, právo, forenznú analýzu, škodlivý softvér a riešenie bezpečnostných incidentov)

Bezpečnosť systémov (bezpečnosť operačných systémov a počítačových sietí)

Kryptológia (kryptológia, elektronický podpis a PKI)

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Jednotlivé bloky sú relatívne nezávislé a záujemca sa môže prihlásiť na hociktorý z nich. Pri prednáškach je počet záujemcov ohraničený veľkosťou miestnosti (max 70 účastníkov).

Výstupom budú prezentácie prednášajúcich a cca 300 stranový učebný podklad, ktoré budú zverejnené na web sídle informatizácia.sk po skončený štúdia.

Prednášky sú určené pre účastníkov verejnej správy. Účasť je bezplatná. Prihlásiť sa je potrebné na e-mail: ivan.vazan@mfsr.sk najneskoršie 10 dní pred predpokladanou účasťou na prednáške. Na prvú prednášku 17.9. 2014 a 18.9 2014 je potrebne sa prihlásiť **do 12.9.2014.**

Registrácia platí až po potvrdení účasti a e-mailovej pozvánky zo strany MF SR. V prípade otázok kontaktujte ivan.vazan@mfsr.sk alebo Tel: 02/59582449

KPMG
cutting through complexity™

5 Harmonogram štúdia

17.9.2014	**Riadenie IB 1.**		
	D.Olejár	Zavedenie Systému manažmentu informačnej bezpečnosti v organizácii	4 hod
	L. Hlavička	Forenzná analýza I.	4 hod
18.9.2014	**Riadenie IB 1.**		
	D.Olejár	Politika IB (Bezpečnostná politika) organizácie	4 hod
	L. Hlavička	Forenzná analýza II.	4 hod
1.10.2014	**Kryptológia 1**		
	M.Stanek	Úvod do kryptológie	2 hod
	O.Grošek	Prehľad kryptoanalýzy	2 hod
	O.Grošek	Postkvantová kryptografia	1 hod
	P.Zajac	Lineárna a diferenciálna kryptoanalýza	3 hod
2.10.2014	**Kryptológia 1**		
	M.Stanek	Symetrické šifry	4 hod
	M.Vojvoda	Kryptoanalýza prúdových šifier	2 hod
	K.Nemoga	Využitie LLL algoritmu pre kryptoanalýzu	2 hod
15.10.2014	**Bezpečnosť systémov 1**		
	J.Janáček	Pokročilé bezpečnostné mechanizmy v OS Linux I.	4 hod
	S.Ivančík	Penetračné testovanie	4 hod
16.10.2014	**M.Jurčík**	Bezpečnostné incidenty	4 hod
	J.Janáček	Pokročilé bezpečnostné mechanizmy v OS Linux II.	4 hod
22.10.2914	**Riadenie IB 2**		
	D.Olejár	Bezpečnostný projekt Informačného systému	4 hod
	L.Hudec	Bezpečnosť v priebehu životného cyklu systému	4 hod
23.10.2914	**D.Olejár**	Kategorizácia informácie a systémov	4 hod
	L.Hudec	Analýza rizík	4 hod
29.10.2014	**Kryptológia 2**		
	M.Stanek	Asymetrické šifry	4 hod
	M.Sýs	Súčasný stav v riešení problému DL a faktorizácie	2 hod

	M. Repka	Útoky cez postranné kanály proti ECC a McEliece algoritmom	2 hod
30.10.2014	**M.Stanek**	Hašovacie funkcie a autentizačné kódy	4 hod
	M.Rjaško	Digitálne podpisy	4 hod

5.11.2014	**Bezpečnosť systémov 2**		
	J.Janáček	Konfiguracia siete, firewall-u, sietovych sluzieb v OS Linux	4 hod
	P.Košinár	Malware 1.	4 hod
6.11.2014	**P.Košinár**	Malware 2	4 hod
	J.Janáček	VPN v OS Linux	4 hod
12.11.2014	**Riadenie IB 3**		
	D.Olejár	Prehľad bezpečnostne relevantnej legis-latívy	4 hod
	L.Hudec	Bezpečnosť bezdrôtových sietí	4 hod
13.11.2014	**L. Hlavička**	Ako sa brániť útokom, nastavenia	4 hod
	L.Hudec	Bezpečnostné brány	4 hod
3.12.2014	**Kryptológia 3**		
	M.Rjaško	Protokoly pre autentizáciu a dohodnutie kľúča	4 hod
	D.Olejár	Elektronický podpis, PKI a CA	4 hod
4.12.2014	**R. Ostertág**	Implementácia	4 hod
	D.Olejár	Zákon o elektronickom podpise	4 hod
10.12.2014	**Bezpečnosť systémov 3**		
	R.Ostertág	Linux vo svete Windows	4 hod
	L.Hudec	DoS a DDoS útoky	4 hod
11.12.2014	**M.Majerčík**	Sieťové prostriedky na vytváranie VPN	4 hod
	L.Hudec	Bezpečnosť virtualizácie a cloud compu-tingu	4 hod

6 Podrobné informácie o programe jednotlivých blokov

Riadenie Informačnej bezpečnosti 1 17. a 18.9.2014 Datacentrum, Bratislava		
Program	**17.9.2014**	
	téma	**Zavedenie Systému manažmentu informačnej bezpečnosti v organizácii**
	vyučujúci	Daniel Olejár
	forma	prednáška
	rozsah	4 hodiny
	čas	8:00 – 11:35
	miestnosť	
	max. počet účastníkov	
	Abstrakt. Zavedenie ISMS v organizácii [*čo je ISMS, prečo organizácia potrebuje ISMS, požiadavky noriem ISO/IEC 27001 a 2 na ISMS. Postup pri zavádzaní ISMS podľa ISO/IEC 27005 a BSI Štandardu 1. Legislatívne požiadavky na riadenie IB v organizácii.*]	
	téma	**Forenzná analýza I.**
	vyučujúci	Lukáš Hlavička
	forma	
	rozsah	4 hodiny
	čas	12:30-16:05
	miestnosť	
	max. počet účastníkov	
	Abstrakt. *Elektronický dôkaz a stopa (definícia, rozdiely oproti fyzickej stope, atribúty, klasifikáca), typy forenzných analýz. Proces forenznej analýzy (získavanie dôkazov, formulácia forenznej hypotézy, analýza dôkazov, reporting), chain of custudy. Súborové systémy a spôsob ukladania dát na média [Súborové systémy FAT32, NTFS, ext4; slackspace, fragmentácia dát, vymazávanie dát] , operačné systémy a ukladanie dát. Získavanie dôkazov, integrita a verifikáciá získaných dát, forenzný obraz pamäte, disku,štandardné a open source nástroje, praktické ukážky. Získavanie dôkazov z nealokovaného miesta a slack space.Získavanie dôkazov zo siete. Analýza dôkazov. Časové pečiatky, súborové fragmenty, registre. Windows 2000/XP/Vista/7 – lokácia informácií a ich využitie. Linux Debian/RedHat – lokácia informácií a ich využitie. Praktická ukážka, fiktívny prípad*	

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Riadenie Informačnej bezpečnosti 1
17. a 18.9.2014
Datacentrum, Bratislava

Program	**18.9.2014**	
	téma	**Politika informačnej bezpečnosti (Bezpečnostná politika) organizácie**
	vyučujúci	Daniel Olejár
	forma	prednáška
	rozsah	4 hodiny
	čas	8:00 – 11:35
	miestnosť	
	max. počet účastníkov	
	Abstrakt. Bezpečnostná politika [*význam bezpečnostnej politiky, obsah bezpečnostnej politiky podľa ISO/IEC 27001 a 2, legislatívne požiadavky na bezpečnostnú politiku (Zákon o ochrane osobných údajov, Výnos MF SR), riešenia/formulácie pre jednotlivé oblasti, ktoré pokrýva bezpečnostná politika, Bezpečnostné štandardy pre jednotlivé oblasti, vypracovanie a správa bezpečnostnej politiky. Vzťah Bezpečnostnej politiky a iných dokumentov organizácie.*]	
	téma	**Forenzná analýza II.**
	vyučujúci	Lukáš Hlavička
	forma	
	rozsah	4 hodiny
	čas	12:30-16:05
	miestnosť	
	max. počet účastníkov	
	Abstrakt. Sieťová forenzná analýza *zachytávanie komunikácie, získanie a analýza dát, MITM, technika HUBIN. Štandardné nástroje, praktická ukážka. RAM, analýza pamäte RAM (platforma windows). Dáta uložené v pamäti (volatilné dáta). extrakcia informácií z pamäte RAM (súbory, šifrovacie kľúče, sieťové spojenia). štandardné nástroje na analýzu pamäte (Volatility), praktická ukážka. Online forenzná analýza a incident response. Fiktívny prípad konkrétnej analýzy*	

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Kryptológia 1 1.10 a 2.10. 2014 Datacentrum, Bratislava		
Program	**1.10.2014**	
	téma	**Úvod do kryptológie**
	vyučujúci	Martin Stanek
	forma	prednáška
	rozsah	2 hodiny
	čas	8:00 – 9:40
	miestnosť	
	max. počet účastníkov	
	Abstrakt. Úvod - pojmy, ciele útokov na kryptografické schémy, prostriedky útočníka,	
	téma	**Prehľad kryptoanalýzy**
	vyučujúci	Otokar Grošek
	forma	prednáška
	rozsah	2 hodiny
	čas	9:55-11:35
	miestnosť	
	max. počet účastníkov	
	Abstrakt. *Evolúcia kryptoanalýzy, Štruktúra jazyka, Základné útoky na vybrané klasické šifry, Počítače a klasické šifry, Československé šifry počas WW2, Šifry s veľmi dlhým kľúčom, Rotorové šifry, princípy a lúštenie, Základné útoky na šifry, Diferenciálna a lineárna kryptoanalýza, Riešenie niektorých ťažkých úloh, Požiadavka z návrhu „AES“ je nereálna, Algebrické metódy, LLL algoritmus, Postranné kanály*	
	téma	**Postkvantová kryptografia**
	vyučujúci	Otokar Grošek
	forma	prednáška
	rozsah	1 hodina
	čas	12:30-13:15
	miestnosť	
	max. počet účastníkov	
	Abstrakt. *Vysvetlime si základne pojmy: PQ počítač a PQ kryptografia, súčasný stav, algoritmy, P ? NP a subexponenciálne algoritmy,.*	
	téma	**Lineárna a diferenciálna kryptoanalýza**
	vyučujúci	Pavol Zajac
	forma	prednáška
	rozsah	3 hodiny
	čas	13:25-16:05
	miestnosť	
	max. počet účastníkov	

KPMG
cutting through complexity™

	Abstrakt. *Jedna z hlavných podmienok pri výbere šifrovacieho štandardu AES bola potreba preukázať odolnosť voči technikám lineárnej a diferenciálnej kryptoanalýzy. V prednáške si predstavíme základný princíp lineárnej a diferenciálnej kryptoanalýzy jednak všeobecne, a jednak na konkrétnej zjednodušenej modelovej šifre (SP sieti). Na záver stručne sumarizujeme dôsledky pre návrh moderných symetrických šifier (špecificky AES).*

Kryptológia 1 1. a 2.10. 2014 Datacentrum, Bratislava		
Program	**2.10.2014**	
	téma	**Symetrické šifry**
	vyučujúci	Martin Stanek
	forma	prednáška
	rozsah	4 hodiny
	čas	8:00 – 11:35
	miestnosť	
	max. počet účastníkov	
	Abstrakt. *Blokove šifry, kaskády a ich bezpečnosť, AES, TDEA, výplne, kradnutie šifrového textu, módy blokových šifier (vlastnosti, silné stránky a slabiny), prúdové šifry, ...*	
	téma	**Kryptoanalýza prúdových šifier**
	vyučujúci	Milan Vojvoda
	forma	prednáška
	rozsah	2 hodiny
	čas	12:30-14:10
	miestnosť	
	max. počet účastníkov	
	Abstrakt. *Prúdový šifrátor a jeho model pre útoky. Lineárny spätnoväzobný register (LFSR). Útok rozdeľuj a panuj (ukážka na Geffeho generátore a šifrách ORYX, A5/1). Korelačné útoky (ukážka na Geffeho generátore). Útok so vzorkami (idea útoku na šifru A5/1).*	
	téma	**Využitie LLL algoritmu pre kryptoanalýzu**
	vyučujúci	Karol Nemoga
	forma	prednáška
	rozsah	2 hodiny
	čas	14:25-16:05
	miestnosť	
	max. počet účastníkov	
	Abstrakt. *História LLL problému. Geometria čísel, diofantické aproximácie. Problematika mrežových bodov, historický vývoj. Problematika optimalizácie, lineárne*	

	programovanie. Problém najkratšieho vektora, najbližšieho vektora. LLL kryptografia. Príklady metód. Ruksakový algoritmus, NTRU kryptosystém. Zložitosť útokov.

Bezpečnosť systémov 1 15. a 16.10. 2014 Datacentrum, Bratislava		
Program	**15.10.2014**	
	téma	**Pokročilé bezpečnostné mechanizmy v OS Linux I.**
	vyučujúci	Jaroslav Janáček, Richard Ostertág
	forma	prednáška
	rozsah	4 hodiny
	čas	8:00 – 11:35
	miestnosť	
	max. počet účastníkov	
	Abstrakt. *capabilities, SELinux*	
	téma	**Penetračné testovanie**
	vyučujúci	Slavomír Ivančík
	forma	prednáška
	rozsah	4 hodiny
	čas	12:30-16:05
	miestnosť	
	max. počet účastníkov	
	Abstrakt. *Princíp penetračného testovania a ukážky z používania niektorých voľne šíriteľných nástrojov ako napríklad NIKTO, BackTrack,...*	

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Bezpečnosť systémov 1 15. a 16.10. 2014 Datacentrum, Bratislava		
Program	**16.10.2014**	
	téma	**Nástroje IDPS**
	vyučujúci	Peter Jurik
	forma	prednáška
	rozsah	4 hodiny
	čas	8:00 – 11:35
	miestnosť	
	max. počet účastníkov	
	Abstrakt. *Špecifikácia open source NIDPS produktov Snort a Suricata spolu s uvedeníme výhod a nevýhod, Ukážky funkcionality snortu, implementácie pravidiel a spracovania výstrah, Ukážky reálnej činnosti snortu pri detekcii niektorých útokov.* *Špecifikácia open source HIDPS produktov OSSEC, fail2ban a DenyHost spolu s opisom ich výhod a nevýhod. Ukážky funkcionality OSSECu, jeho možností detekcie a spracovania výstrah, Ukážkyreálnej činnosti OSSECu pri detekcii niektorých útokov.* *Stručný úvod do SIEM, SEM technológií, Špecifikácia open source produktu OSSIM, Ukážky funkcionality OSSIMu, spracovania, korelácie a vyhodnocovania eventov*	
	téma	**Pokročilé bezpečnostné mechanizmy v OS Linux II.**
	vyučujúci	Jaroslav Janáček, Richard Ostertág
	forma	prednáška
	rozsah	4 hodiny
	čas	12:30-16:05
	miestnosť	
	max. počet účastníkov	
	Abstrakt. capabilities, SELinux	

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Riadenie informačnej bezpečnosti 2 22. a 23.10. 2014 Datacentrum, Bratislava		
Program	**22.10.2014**	
	téma	**Bezpečnostný projekt Informačného systému**
	vyučujúci	Daniel Olejár
	forma	prednáška
	rozsah	4 hodiny
	čas	8:00 – 11:35
	miestnosť	
	max. počet účastníkov	
	Abstrakt. *úloha bezpečnostného projektu, obsah bezpečnostného projektu podľa NIST a BSI, Protection profile a Security target normy ISO/IEC 15408, Common Criteria, požiadavky slovenskej legislatívy na bezpečnostný projekt. Zákon o kritickej infraštruktúre, Zákon o ochrane osobných údajov, Zákon o ISVS, Výnos MF SR. Vzťah Bezpečnostnej politiky a bezpečnostného projektu systému. Bezpečnostný projekt a ISMS. Zmeny/úpravy bezpečnostného projektu. Vzorový bezpečnostný projekt*	
	téma	**Bezpečnosť v priebehu životného cyklu systému**
	vyučujúci	Ladislav Hudec
	forma	prednáška
	rozsah	4 hodiny
	čas	12:30-16:05
	miestnosť	
	max. počet účastníkov	
	Abstrakt. *Špecifikácia bezpečnostných požiadaviek na systém, protection profile, vývoj, implementácia, testovanie, akceptačné konanie, schválenie/nasadenie, implementácia bezpečnostných opatrení, opravy chýb, prevádzka, zmeny, vyradenie systému. Právne aspekty. Outsourcing. Vzdialená správa.*	

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Riadenie informačnej bezpečnosti 2 22. a 23.10. 2014 Datacentrum, Bratislava		
Program	**23.10.2014**	
	téma	**Kategorizácia informácie a systémov**
	vyučujúci	Daniel Olejár
	forma	prednáška
	rozsah	4 hodiny
	čas	8:00 – 11:35
	miestnosť	
	max. počet účastníkov	
	Abstrakt. *Význam klasifikácie. Vzťah klasifikácie a analýzy rizík. Kritériá klasifikácie. Metodika FIPS 199. Dôvernosť, integrita, dostupnosť, autentickosť. Závažnosť dopadu. Klasifikácia informácie. Klasifikácia systémov. Typy informácie podľa slovenskej legislatívy a požiadavky na jej ochranu. Porovnanie s FIPS 199. Opatrenia pre jednotlivé kategórie systémov.*	
	téma	**Analýza rizík**
	vyučujúci	Ladislav Hudec
	forma	prednáška
	rozsah	4 hodiny
	čas	12:30-16:05
	miestnosť	
	max. počet účastníkov	
	Abstrakt. *Analýza a správa rizík podľa ISO/IEC 27005*	

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Kryptológia 2 29. a 30.10. 2014 Datacentrum, Bratislava		
Program	**29.10.2014**	
	téma	**Asymetrické šifry**
	vyučujúci	Martin Stanek
	forma	prednáška
	rozsah	4 hodiny
	čas	8:00 – 11:35
	miestnosť	
	max. počet účastníkov	
	Abstrakt. *základné problémy pre asym. konštrukcie, RSA, DLOG a eliptické krivky a pod., schémy pre šifrovanie kľúčov, výplne (napr. RSA-OAEP), implementačné otázky a pod.*	
	téma	**Súčasný stav v riešení problému DL a faktorizácie**
	vyučujúci	Marek Sýs
	forma	prednáška
	rozsah	2 hodiny
	čas	12:30-14:10
	miestnosť	
	max. počet účastníkov	
	Abstrakt. *Prednáška je zameraná na dva hlavné stavebné kamene kryptografie verejného kľúča - problém faktorizácie a problém diskrétneho logaritmu. V prednáške sa dozviete základné rozdelenie metód (Number Field Sieve, Multiple Number Field, Special Number Field Sieve, Function Field Sieve a iné) riešiacich uvedené problémy. Predstavíme tu hlavné myšlienky uvedených metód, ich zložitosť a ich dopad na bezpečné parametre šifier verejného kľúča ako RSA, ElGamal, Diffie–Hellman a iných.*	
	téma	**Útoky cez postranné kanály proti ECC a McEliece algoritmom**
	vyučujúci	Marek Repka
	forma	prednáška
	rozsah	2 hodiny
	čas	14:25-16:05
	miestnosť	
	max. počet účastníkov	
	Abstrakt. *V úvode do postranných kanálov budú prezentované definície postranných kanálov a únikov informácií. Útoky postrannými kanálmi budú kategorizované podľa prístupu k zariadeniu a možnosťami manipulácie s nim. Budú tiež spomenuté príklady Útokov postrannými kanálmi z praxe. Budú načrtnuté protiopatrenia a*	

KPMG
cutting through complexity™

	ich kategorizácie. *Po úvode nasleduje analýza postranných kanálov na eliptických krivkách. Budú ukázané operačné, ako aj dátové závislosti. Budú demonštrované nesprávne prístupy na aplikovanie protiopatrení, ako aj tie účinné. Bude prezentovaný nebezpečný útok na Elektronický podpis ECDSA.* *Z rovnakého hľadiska bude rozobraný aj post-qvantový McEliece kryptosystém s verejným kľúčom.*

Kryptológia 2 29. a 30.10. 2014 Datacentrum, Bratislava		
Program	**30.10.2014**	
	téma	**Hašovacie funkcie a autentizačné kódy**
	vyučujúci	Martin Stanek
	forma	prednáška
	rozsah	4 hodiny
	čas	8:00 – 11:35
	miestnosť	
	max. počet účastníkov	
	Abstrakt. *základné problémy pre asym. konštrukcie, RSA, DLOG a eliptické krivky a pod., schémy pre šifrovanie kľúčov, výplne (napr. RSA-OAEP), implementačné otázky a pod.*	
	téma	**Digitálne podpisy**
	vyučujúci	Michal Rjaško
	forma	prednáška
	rozsah	4 hodiny
	čas	12:30-16:05
	miestnosť	
	max. počet účastníkov	
	Abstrakt. *schémy pre digitálne podpisy, RSA, (EC) DSA, RSA-PSS, očakávané vlastnosti (def. bezpečnosti), implementačné otázky*	

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Bezpečnosť systémov 2 5. a 6.11. 2014 Datacentrum, Bratislava		
Program	**5.11.2014**	
	téma	**Konfigurácia siete, firewall-u, sieťových služieb v OS Linux**
	vyučujúci	Jaroslav Janáček, Richard Ostertág
	forma	prednáška
	rozsah	4 hodiny
	čas	8:00 – 11:35
	miestnosť	
	max. počet účastníkov	
	Abstrakt. *V rámci prednášky sa pozrieme na konfiguráciu siete a sieťových služieb v OS Linux. Špeciálne sa zameriame na pokročilé techniky ako Policy routing, firewall, NAT, SELinux.*	
	téma	Malware 1.
	vyučujúci	Peter Košinár
	forma	prednáška
	rozsah	4 hodiny
	čas	12:30-16:05
	miestnosť	
	max. počet účastníkov	
	Abstrakt. *Podstata malware, typy, prejavy, obrana pred malware, trendy vo vývoji malware.*	

KPMG
cutting through complexity™

Bezpečnosť systémov 2 5. a ž.11. 2014 Datacentrum, Bratislava		
Program	**6.11.2014**	
	téma	Malware 2
	vyučujúci	Peter Košinár
	forma	prednáška
	rozsah	4 hodiny
	čas	8:00 – 11:35
	miestnosť	
	max. počet účastníkov	
	Abstrakt. *Podstata malware, typy, prejavy, obrana pred malware, trendy vo vývoji malware.*	
	téma	**VPN v OS Linux**
	vyučujúci	Jaroslav Janáček
	forma	prednáška
	rozsah	4 hodiny
	čas	12:30-16:05
	miestnosť	
	max. počet účastníkov	
	Abstrakt. *V rámci prednášky dokončíme témy z Konfigurácie siete a Pokročilých bezp. mechanizmov v OS Linux. Následne sa pozrieme na vybrané technológie VPN v OS Linux, konkrétne sa zameriame na OpenVPN a IPSec.*	

Ministerstvo financií Slovenskej republiky

EFQM Recognised for excellence 5 star - 2012

Riadenie informačnej bezpečnosti 3 12. a 13.11. 2014 Datacentrum, Bratislava		
Program	**12.11. 2014**	
	téma	**Prehľad bezpečnostne relevantnej legislatívy**
	vyučujúci	Daniel Olejár
	forma	prednáška
	rozsah	4 hodiny
	čas	8:00 – 11:35
	miestnosť	
	max. počet účastníkov	
	Abstrakt. Prehľad slovenských zákonov, vyhlášok a štandardov stanovujúcich povinnosti v oblasti informačnej bezpečnosti *[Zákon o ochrane osobných údajov, Zákon o ochrane utajovaných skutočností, Zákon o ISVS, Výnos MF o štandardoch, Zákon o kritickej infraštruktúre, Zákon o elektronickom podpise, Zákon o slobodnom prístupe k informáciám, Trestný zákon, Autorský zákon, Telekomunikačný zákon, Zákon o bankách, Zákon o e-Gov, ... povinnosti z nich vyplývajúce a spôsob ich riešenia.*	
	téma	**Bezpečnosť bezdrôtových sietí**
	vyučujúci	Ladislav Hudec
	forma	prednáška
	rozsah	4 hodiny
	čas	12:30-16:05
	miestnosť	
	max. počet účastníkov	
	Abstrakt. *Bezpečnosť bezdrôtových sietí WLAN IEEE 802.11i, bezpečnosť bezdrôtovej transportnej vrstvy, protokol WAP (end-to-end bezpečnosť). Príklady riešení bezdrôtových sietí*	

KPMG cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Riadenie informačnej bezpečnosti 3 11. a 12.11. 2014 Datacentrum, Bratislava		
Program	**13.11. 2014**	
	téma	**Ako sa brániť útokom, nastavenia**
	vyučujúci	L. Hlavička
	forma	prednáška
	rozsah	4 hodiny
	čas	8:00 – 11:35
	miestnosť	
	max. počet účastníkov	
	Abstrakt.	
	téma	**Bezpečnostné brány**
	vyučujúci	Ladislav Hudec
	forma	prednáška
	rozsah	4 hodiny
	čas	12:30-16:05
	miestnosť	
	max. počet účastníkov	
	Abstrakt. *Charakteristiky bezpečnostných brán, typy bezpečnostných brán, hosťovanie bezpečnostných brán, umiestnenie bezpečnostnej brány. Príklady riešení (Paketovy filter v OS Linux, Voľne šíriteľná bezpečnostná brána)*	

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Kryptológia 3 3. a 4.12. 2014 Datacentrum, Bratislava		
Program	**3.12.2014**	
	téma	**Protokoly pre autentizáciu a dohodnutie kľúča**
	vyučujúci	M.Rjaško
	forma	prednáška
	rozsah	4 hodiny
	čas	8:00 – 11:35
	miestnosť	
	max. počet účastníkov	
	Abstrakt. *základné pojmy, časové pečiatky, príležitostné slová, dôveryhodný server, typy útokov na protokoly (zrkadlenie, útočník uprostred, atď.), DH protokol, SSL/TLS (príp. iné)*	
	téma	**Elektronický podpis, PKI a CA**
	vyučujúci	Daniel Olejár
	forma	prednáška
	rozsah	4 hodiny
	čas	12:30-16:05
	miestnosť	
	max. počet účastníkov	
	Abstrakt *bezpečnostné funkcie digitálneho podpisu, vlastnoručný a elektronický podpis, certifikát verejného kľúča a jeho úloha, revokácia certifikátov, overovanie platnosti certifikátov, CRL, RA, CA a ich úlohy, vydávanie certifikátov, časové pečiatky, atribútové certifikáty, PKI, hierarchická PKI, koreňová CA, mesh PKI, krížové certifikáty, bridge CA, bezpečnosť elektronického podpisu, normy*	

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Kryptológia 3 3. a 4.12. 2014 Datacentrum, Bratislava		
Program	**4.12.2014**	
	téma	**Implementácia**
	vyučujúci	Richard Ostertág
	forma	prednáška
	rozsah	4 hodiny
	čas	8:00 – 11:35
	miestnosť	
	max. počet účastníkov	
	Abstrakt. *výkon kryptografických konštrukcií, porovnania dĺžok kľúčov, heslá a ich ukladanie, útoky súvisiace s implementáciou - dúhové tabuľky, postranné kanály (timing útok a pod.), príklady implementačných zraniteľností + ďalšie drobnosti (zdieľanie tajomstva a pod.)*	
	téma	**Elektronický podpis, PKI a CA**
	vyučujúci	Daniel Olejár
	forma	prednáška
	rozsah	4 hodiny
	čas	12:30-16:05
	miestnosť	
	max. počet účastníkov	
	Abstrakt *komentáre k zákonu a vyhláškam – technologická interpretácia právnych požiadaviek*	

KPMG
cutting through complexity™

Ministerstvo financií Slovenskej republiky

EFQM Recognised for excellence 5 star - 2012

Bezpečnosť systémov 3 10. a 11.12. 2014 Datacentrum, Bratislava		
Program	**10.12.2014**	
	téma	**Linux vo svete Windows**
	vyučujúci	Jaroslav Janáček, Richard Ostertág
	forma	prednáška
	rozsah	4 hodiny
	čas	8:00 – 11:35
	miestnosť	
	max. počet účastníkov	
	Abstrakt.	
	téma	**DoS a DDoS útoky**
	vyučujúci	Ladislav Hudec
	forma	prednáška
	rozsah	4 hodiny
	čas	12:30-16:05
	miestnosť	
	max. počet účastníkov	
	Abstrakt. *typy DoS a DDoS útokov. Botnety, všeobecné pravidlá ochrany, prostriedky ochrany proti DoS a DDoS útokom*	

KPMG cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Bezpečnosť systémov 3 10. a 11..12. 2014 Datacentrum, Bratislava		
Program	**11.12.2014**	
	téma	**Sieťové prostriedky na vytváranie VPN**
	vyučujúci	Michal Majerčík
	forma	prednáška
	rozsah	4 hodiny
	čas	8:00 – 11:35
	miestnosť	
	max. počet účastníkov	
	Abstrakt. *charakteristiky zariadení popredných výrobcov na vytvorenie VPN, demonštrácia príkladov použitia zariadení (napríklad CISCO a iní)*	
	téma	**Bezpečnosť virtualizácie a cloud computingu**
	vyučujúci	Ladislav Hudec
	forma	prednáška
	rozsah	4 hodiny
	čas	12:30-16:05
	miestnosť	
	max. počet účastníkov	
	Abstrakt. *Virtualizované systémy:* *- bezpečnostné otázky pri hardvérovej virtualizácii* *- prehľad virtualizačných konceptov* *- model hrozieb* *- detekcia virtuálneho stroja* *- kompromitácia hostiteľa, operačného systému hosta, hypervisora, interfejsu manažmentu, siete* *- bezpečnostné protiopatrenia* *Cloudové počítanie:* *- základy a architektúra* *- základy softvérovej bezpečnosti* *- rizika a bezpečnostne výzvy* *- bezpečnostná architektúra, otázky životného cyklu*	

KPMG
cutting through complexity™