

Studijní plán

Název plánu: Open Informatics - Cyber Security

Sou část VUT (fakulta/ústav/další): Fakulta elektrotechnická

Katedra: katedra počítačové grafiky a interakce

Obor studia, garantovaný katedrou:

Garant oboru studia.: doc. Ing. David Šišlák, Ph.D.

Program studia: Open Informatics

Typ studia: Navazující magisterské prezenční

Předepsané kredity: 85

Kredity z volitelných předmětů: 35

Kredity v rámci plánu celkem: 120

Poznámka k plánu:

Název bloku: Povinné předměty programu

Minimální počet kreditů bloku: 49

Role bloku: P

Kód skupiny: 2018_MOIEP

Název skupiny: Compulsory subjects of the programme

Podmínka kredity skupiny: V této skupině musíte získat 24 kredit

Podmínka předmětů skupiny: V této skupině musíte absolvovat 4 předměty

Kredity skupiny: 24

Poznámka ke skupině:

Kód	Název předmětu / Název skupiny předmětů (u skupiny předmětů seznam kód jejich členů) Využíjí, autoři a garantů (gar.)	Zakonění	Kredity	Rozsah	Semestr	Role
BE4M33PAL	Advanced Algorithms Marko Genyk-Berezovskij, Daniel Prša Daniel Prša Daniel Prša (Gar.)	Z,ZK	6	2P+2C	Z	P
BE4M35KO	Combinatorial Optimization	Z,ZK	6	3P+2C	L	P
BE4MSVP	Software or Research Project Petr Pošík, Jaroslav Sloup, Katarína Ākušová Katarína Ākušová	KZ	6		Z,L	P
BE4M01TAL	Theory of Algorithms	Z,ZK	6	3P+2S	L	P

Charakteristiky předmětů této skupiny studijního plánu: Kód=2018_MOIEP Název=Compulsory subjects of the programme

BE4M33PAL	Advanced Algorithms	Z,ZK	6
Basic graph algorithms and graph representation. Combinatorial algorithms. Application of formal languages theory in computer science - pattern matching.			
BE4M35KO	Combinatorial Optimization	Z,ZK	6
The goal is to show the problems and algorithms of combinatorial optimization (often called discrete optimization; there is a strong overlap with the term operations research). Following the courses on linear algebra, graph theory, and basics of optimization, we show optimization techniques based on graphs, integer linear programming, heuristics, approximation algorithms and state space search methods. We focus on application of optimization in stores, ground transportation, flight transportation, logistics, planning of human resources, scheduling in production lines, message routing, scheduling in parallel computers.			
BE4MSVP	Software or Research Project	KZ	6
Samostatná práce na problému-projektu pod vedením školitele. V rámci tohoto předmětu je možné (obvyklé) řešit dílčí problém diplomové práce. Proto doporučujeme zvolit si téma diplomové práce již po ústředním 3. semestru a jeho výsledky nepodcenit. Absolování předmětu softwarový a výzkumný projekt musí mít jasně definovaný výstup, například technickou zprávu či programový produkt, který je ohodnocen klasifikovaným zápočtem. Důležité upozornění: - Standardně není možné absolvovat více než jeden předmět tohoto typu. - Výjimkou může být i jiný garant hlavního (major) oboru. Možný důvod pro udělení výjimky je, že práce-projekt má jiné téma a je vedena jiným vedoucím. Typickým příkladem může být práce na projektu v zahraničí. Poznámka: Student si předmět SVP zapisuje na katedře vedoucího práce. Pokud ta předmět nevypíše, pak na katedře 13139 (varianta A4M39SVP) Kontaktní email v případě dalších dotazů: oi@fel.cvut.cz Bližší pokyny k zadání a vypracování projektu naleznete na stránkách katedry počítačové grafiky a interakce http://dcgi.felk.cvut.cz/cs/study/predmetprojekt . Projekt je v rámci předmětu obhajován. Výsledek studentské ankety předmětu je zde: http://www.fel.cvut.cz/anketa/aktualni/courses/A4M39SVP			
BE4M01TAL	Theory of Algorithms	Z,ZK	6
Předmět seznamuje se základními pojmy a postupy teorie složitosti. Důraz je kladen na časovou složitost, ale studenti se seznámí i s paměťovou složitostí a amortizovanou složitostí. Studenti se seznámí s Turingovými stroji a to jak s jednou, tak i více páskami. Je uveden pojem redukce úlohy/jazyka a polynomiální redukce jazyka/úlohy. Předmět se věnuje i známým složitostem P, NP, NPC, co-NP, a i známým PSPACE a NPSpace založeným na paměťové složitosti. Je uvedena Savitchova věta. Dále se předmět věnuje pravděpodobnostním algoritmům a i známým RP a ZPP. Na závěr se studenti seznámí s teorií nerozhodnutelnosti. K pochopení látky se též používají konkrétní algoritmy, jedná se hlavně o algoritmy z teorie grafů a kryptografie.			

Kód skupiny: 2018_MOIEDIP

Název skupiny: Diplomová práce - Diploma Thesis

Podmínka kredity skupiny: V této skupině musíte získat 25 kredit

Podmínka p edm ty skupiny: V této skupin musíte absolvovat 1 p edm t

Kredity skupiny: 25

Poznámka ke skupině:

Kód	Název p edm tu / Název skupiny p edm t (u skupiny p edm t seznam kód jejích len) Vyu ující, auto i a garanti (gar.)	Zakon ení	Kredity	Rozsah	Semestr	Role
BDIP25	Diplomová práce - Diploma Thesis	Z	25	22s	L	P

Charakteristiky p edmet této skupiny studijního plánu: Kód=2018_MOIEDIP Název=Diplomová práce - Diploma Thesis

BDIP25	Diplomová práce - Diploma Thesis	Z	25
--------	----------------------------------	---	----

Samostatná záv re ná práce inženýrského studia komplexního charakteru. Téma práce si student vybere z nabídky témat souvisejících se studovaným oborem, která vypíše oborová katedra i katedry. Práce bude obhajována p ed komisí pro státní záv re né zkoušky.

Název bloku: Povinné p edm ty oboru

Minimální po et kredit bloku: 36

Role bloku: PO

Kód skupiny: 2018_MOIEPO2

Název skupiny: Compulsory subjects of the branch

Podmínka kredity skupiny: V této skupin musíte získat 36 kredit

Podmínka p edm ty skupiny: V této skupin musíte absolvovat 6 p edm t

Kredity skupiny: 36

Poznámka ke skupině:

Kód	Název p edm tu / Název skupiny p edm t (u skupiny p edm t seznam kód jejích len) Vyu ující, auto i a garanti (gar.)	Zakon ení	Kredity	Rozsah	Semestr	Role
BE2M32PST	Advanced Networking Technologies Leoš Bohá Zbyn k Kocur Leoš Bohá (Gar.)	Z,ZK	6	2P + 2L	Z,L	PO
BE4M36KBE	Communications Security	Z,ZK	6	3P+2C	Z	PO
BE4M36BSY	Introduction to Computer Security Tomáš Pevný Tomáš Pevný Tomáš Pevný (Gar.)	Z,ZK	6	2P+2C	Z	PO
BE4M01MKR	Mathematical Cryptography	Z,ZK	6	4P+2S	L	PO
BE4M36ZKS	Software Quality Assurance Miroslav Bureš, Karel Frajták, Václav Rechtberger Miroslav Bureš Miroslav Bureš (Gar.)	Z,ZK	6	2P+2C	Z	PO
BE4M36SAN	Statistical data analysis Ji í Kléma Ji í Kléma Ji í Kléma (Gar.)	Z,ZK	6	2P+2C	Z	PO

Charakteristiky p edmet této skupiny studijního plánu: Kód=2018_MOIEPO2 Název=Compulsory subjects of the branch

BE2M32PST	Advanced Networking Technologies	Z,ZK	6
-----------	----------------------------------	------	---

Subject Advanced Network Technologies extends student knowledge in an area of modern network technologies. The course strives to deepen student's knowledge in more advanced technical features of contemporary networking protocols in data networks. Students will get hands-on experience with topics like Internet unicast routing, multicast routing, IPv6 and design of MPLS networks using various network simulation tools.

BE4M36KBE	Communications Security	Z,ZK	6
-----------	-------------------------	------	---

P edm t p edstavuje student m problematiku komunika ních protokol používaných pro zabezpe ení komunikace v informa ních systémech. eší zejména otázky spojené s použitím kryptografických protokol pro zabezpe ení d v rnosti komunikace, pro zajišt ní integrity, autentifikaci, autorizaci a dalších vlastností a operací bezpečného SW. Zvláštní z etel je v nován útok m na protokoly, pochopení obecných princip použití protokol pro návrh systému a bezpečnostním implikacím volby protokolu a parametr .

BE4M36BSY	Introduction to Computer Security	Z,ZK	6
-----------	-----------------------------------	------	---

Cílem p edm tu je seznámit poslucha e se sou asnými bezpečnostními riziky opera ních systém a webových aplikací, mezi které pat í například získávání p ístupu p es sí a eskalace práv. Poslucha i získají p ehled o zásadách administrace opera ních systém pro minimalizaci bezpečnostních rizik, o psaní bezpečných aplikací a ov ení jejich bezpečnosti, o nastavování firewall a o forenzní analýze už napadených systém .

BE4M01MKR	Mathematical Cryptography	Z,ZK	6
-----------	---------------------------	------	---

P ednáška vybuduje matematické základy moderní kryptografie (RSA, El-Gamal, šifrování na eliptických k ivkách, hashování) a související algoritmy pro testování prvo ísel (íselná síta) a hledání diskrétního logaritmu.

BE4M36ZKS	Software Quality Assurance	Z,ZK	6
-----------	----------------------------	------	---

Cílem p edm tu je seznámit studenty s technikami testování a zajišt ní kvality software. Po úvodu do metodiky testování si studenti osvojí techniky pro vytvá ení test z modelu aplikace, které jsou základem návrhu jak manuálních, tak automatických test . Poté se nau í vytvá et efektivní jednotkové testy kódu a seznámí se s technikami automatického testování na r zných úrovních. Záv re ná ást p edm tu se poté zabývá úvodem do formálních verifikací vytvá eného software.

BE4M36SAN	Statistical data analysis	Z,ZK	6
-----------	---------------------------	------	---

Cílem p edm tu je seznámit se se statistickými p ístupy k analýze dat nad rámec tradi ní výuky statistiky a pravd podobnosti. Kurz se soust edí na vícepr íznakovou explorativní statistickou analýzu, prohloubí ale i znalosti konfirma ních p ístup .

Název bloku: Volitelné p edm ty

Minimální po et kredit bloku: 0

Role bloku: V

Kód skupiny: 2018_MOIEVOL

Název skupiny: Elective subjects

Podmínka kredity skupiny:

Podmínka p edm ty skupiny:

Kredity skupiny: 0

Poznámka ke skupině: ~Student can choose arbitrary subject of the magister's program (EEM - Electrical Engineering, Power Engineering and Management, EK - Electronics and Communications, KYR - Cybernetics and Robotics, OI - Open Informatics, OES - Open Electronics Systems) which is not part of his curriculum. Student can choose with consideration of recommendation of the branch guarantee. You can find a selection of optional courses organized by the departments on the web site <http://www.fel.cvut.cz/cz/education/volitelne-predmety.html>

Seznam p edm t tohoto pr chodu:

Kód	Název p edm tu	Zakon ení	Kredity
BDIP25	Diplomová práce - Diploma Thesis	Z	25
Samostatná záv re ná práce inženýrského studia komplexního charakteru. Téma práce si student vybere z nabídky témat souvisejících se studovaným oborem, která vypíše oborová katedra i katedry. Práce bude obhajována p ed komisí pro státní záv re né zkoušky.			
BE2M32PST	Advanced Networking Technologies	Z,ZK	6
Subject Advanced Network Technologies extends student knowledge in an area of modern network technologies. The course strives to deepen student's knowledge in more advanced technical features of contemporary networking protocols in data networks. Students will get hands-on experience with topics like Internet unicast routing, multicast routing, IPv6 and design of MPLS networks using various network simulation tools.			
BE4M01MKR	Mathematical Cryptography	Z,ZK	6
P ednáška vybuduje matematické základy moderní kryptografie (RSA, El-Gamal, šifrování na eliptických k ivkách, hashování) a související algoritmy pro testování prvo ísel (íselná síta) a hledání diskrétního logaritmu.			
BE4M01TAL	Theory of Algorithms	Z,ZK	6
P edm t seznamuje se základními pojmy a postupy teorie složitosti. D raz je kladen na asovou složitost, ale studenti se seznámí i pam ovou složitostí a amortizovanou složitostí. Studenti se seznámí s Turingovými stroji a to jak s jednou, tak i více páskami. Je uveden pojem redukce úlohy/jazyka a polynomiální redukce jazyka/úlohy. P edm t se v nuje t ídám složitosti P, NP, NPC, co-NP, a t ídám PSPACE a NPSpace založeným na pam ové složitosti. Je uvedena Savitchova v ta. Dále se p edm t v nuje pravd podobnostním algoritmem a t ídám RP a ZPP. Na záv r se studenti seznámí s teorií nerozhodnutelnosti. K pochopení látky se též používají konkrétní algoritmy, jedná se hlavn o algoritmy z teorie graf a kryptografie.			
BE4M33PAL	Advanced Algorithms	Z,ZK	6
Basic graph algorithms and graph representation. Combinatorial algorithms. Application of formal languages theory in computer science - pattern matching.			
BE4M35KO	Combinatorial Optimization	Z,ZK	6
The goal is to show the problems and algorithms of combinatorial optimization (often called discrete optimization; there is a strong overlap with the term operations research). Following the courses on linear algebra, graph theory, and basics of optimization, we show optimization techniques based on graphs, integer linear programming, heuristics, approximation algorithms and state space search methods. We focus on application of optimization in stores, ground transportation, flight transportation, logistics, planning of human resources, scheduling in production lines, message routing, scheduling in parallel computers.			
BE4M36BSY	Introduction to Computer Security	Z,ZK	6
Cílem p edm tu je seznámit poslucha e se sou asnými bezpečnostními riziky opera ních systém a webových aplikací, mezi které pat í nap íklad získávání p ístupů p es sí a eskalace práv. Poslucha í získají p ehled o zásadách administrace opera ních systém pro minimalizaci bezpečnostních rizik, o psaní bezpečných aplikací a ov ení jejich bezpečnosti, o nastavování firewall a o forenzní analýze už napadených systém .			
BE4M36KBE	Communications Security	Z,ZK	6
P edm t p edstavuje student m problematiku komunika ních protokol používaných pro zabezpeč ení komunikace v informa ních systémech. eší zejména otázky spojené s použitím kryptografických protokol pro zabezpeč ení d v rnosti komunikace, pro zajištění integrity, autentifikaci, autorizaci a dalších vlastností a operací bezpečného SW. Zvláštní z etel je v nován útok m na protokoly, pochopení obecných princip použití protokol pro návrh systému a bezpečnostním implikacím volby protokolu a parametr .			
BE4M36SAN	Statistical data analysis	Z,ZK	6
Cílem p edm tu je seznámit se se statistickými p ístupy k analýze dat nad rámec tradi ní výuky statistiky a pravd podobnosti. Kurz se soust edí na vícepr íznakovou explorativní statistickou analýzu, prohloubí ale i znalosti konfirma ních p ístup .			
BE4M36ZKS	Software Quality Assurance	Z,ZK	6
Cílem p edm tu je seznámit studenty s technikami testování a zajištění kvality software. Po úvodu do metodiky testování si studenti osvojí techniky pro vytvá ení test z modelu aplikace, které jsou základem návrhu jak manuálních, tak automatických test . Poté se nau í vytvá et efektivní jednotkové testy kódu a seznámí se s technikami automatického testování na r zných úrovních. Záv re ná ást p edm tu se poté zabývá úvodem do formálních verifikací vytvá eného software.			
BE4MSVP	Software or Research Project	KZ	6
Samostatná práce na problému-projektu pod vedením školitele. V rámci tohoto p edm tu je možné (obvyklé) ešit díl í problém diplomové práce. Proto doporu ujeme zvolit si téma diplomové práce již po átkem 3. semestru a jeho v asný výb r nepodcenit. Absolovování p edm tu softwarový a výzkumný projekt musí mít jasn definovaný výstup, nap íklad technickou zprávu í programový produkt, který je ohodnocen klasifikovaným zápo tem. D ležitě upozorn í: - Standardn není možné absolovat více než jeden p edm t tohoto typu. - Výjimku m že ud lit garant hlavního (major) oboru. Možný d vod pro ud lení výjimky je, že práce-projekt má jiné téma a je vedena jiným vedoucím. Typickým p íkladem m že být práce na projektu v zahrani í. Poznámka: Student si p edm t SVP zapisuje na kated e vedoucí práce. Pokud ta p edm t nevyvíší, pak na kated e 13139 (varianta A4M39SVP) Kontaktní email v p ípad dalších dotaz : oi@fel.cvut.cz Bližší pokyny k zadání a vypracování projektu naleznete na stránkách katedry po íta ové grafiky a interakce http://dcgi.felk.cvut.cz/cs/study/predmetprojekt . Projekt je v rámci p edm tu obhajován. Výsledek studentské ankety p edm tu je zde: http://www.fel.cvut.cz/anketa/aktualni/courses/A4M39SVP			

Aktualizace výše uvedených informací naleznete na adrese <http://bilakniha.cvut.cz/cs/f3.html>

