Studijní plán

Název plánu: Quantum Informatics

Součást ČVUT (fakulta/ústav/další): Fakulta informačních technologií
Katedra:
Obor studia, garantovaný katedrou:
Garant oboru studia.: prof. Ing. Róbert Lórencz, CSc.
Program studia: Quantum Informatics
Typ studia: Navazující magisterské prezenční
Předepsané kredity: 120
Kredity z volitelných předmětů: 0
Kredity v rámci plánu celkem: 120
Poznámka k plánu:

Název bloku: Povinné předměty programu
Minimální počet kreditů bloku: 96
Role bloku: PP

Kód skupiny: QNIE-PP
Název skupiny: Compulsory courses of the Quantum Informatics
Podmínka kredity skupiny: V této skupině musíte získat 96 kreditů
Podmínka předměty skupiny: V této skupině musíte absolvovat 12 předmětů
Kredity skupiny: 96
Poznámka ke skupině:

Kód	Název předmětu / Název skupiny předmětů *(u skupiny předmětů seznam kódů jejích členů)* *Vyučující,* ***autoři*** *a garanti (gar.)*	Zakončení	Kredity	Rozsah	Semestr	Role
QNIE-DIP	**Diploma Thesis**	Z	30	270ZP	L,Z	PP
QNIE-KKP	**Kryptologie a kvantové počítání** ***Róbert Lórencz***	Z,ZK	6	2P+2C		PP
BQM32KOS	**Kvantové optické komunikace a sítě** *Jiří Weiss, Václav Prajzler, Jan Voves, Leoš Boháč* ***Jiří Weiss*** *Leoš Boháč (Gar.)*	Z,ZK	6	2P+2L	L	PP
QNIE-QC1	**Kvantové výpočty 1**	Z,ZK	6	2P+2C	Z	PP
QNIE-QC2	**Kvantové výpočty 2**	Z,ZK	6	2P+2C	L	PP
QNIE-LOM	**Lineární optimalizace a metody** *Dušan Knop* ***Dušan Knop*** *Dušan Knop (Gar.)*	Z,ZK	5	2P+1C	Z	PP
QNIE-MPR	**Magisterský projekt** ***Zdeněk Muzikář***	Z	7		Z,L	PP
QNIE-MQI	**Matematika pro kvantovou informatiku**	Z,ZK	6	2P+2C	Z	PP
QNIE-PPS	**Programování paralelních systémů**	Z,ZK	6	2P+2C		PP
QNIE-TIN	**Teorie informace**	Z,ZK	6	2P+2C	L	PP
QNIE-CPX	**Teorie složitosti** ***Dušan Knop*** *Dušan Knop (Gar.)*	Z,ZK	6	3P+1C	Z	PP
QNIE-UKT	**Úvod do kvantové teorie**	Z,ZK	6	2P+2C	Z	PP

Charakteristiky předmětů této skupiny studijního plánu: Kód=QNIE-PP Název=Compulsory courses of the Quantum Informatics

QNIE-DIP	Diploma Thesis	Z	30

Independent work of the student under the guidance of the thesis supervisor. Teaching is based on individual consultations with the thesis supervisor or other consultants. The scope of teaching 30 ECTS (i.e. about 900 hours) includes consultations, preparation of theoretical and practical parts of the thesis, writing, preparation for defence and defence of the thesis before the commission. The course supervisor guarantees the quality of the Masters thesis assignment and its compliance with the graduate profile.

QNIE-KKP	Kryptologie a kvantové počítání	Z,ZK	6

The course covers methods and algorithms of cryptology and their relation to quantum computing. In the first introductory lectures, students will be introduced to the basic principles and algorithms of cryptography. Following these topics, students will be introduced to basic cryptanalytic methods. Then some cryptanalytic algorithms running on quantum computers will be presented. In this context, the problem of security of related cryptographic schemes will be discussed. The next lectures will be devoted to post-quantum algorithms. The last lectures deal with cryptosystems using quantum phenomena.

BQM32KOS	Kvantové optické komunikace a sítě	Z,ZK	6

Cílem kurzu je poskytnout komplexní, inženýrský vhled do problematiky optických komunikací se zaměřením na kvantovou distribuci klíče (QKD). Předmět boří hranice mezi tradičními disciplínami a integruje znalosti z vlnové optiky, hardwarové architektury a síťové bezpečnosti. Studenti se naučí chápat komunikační systém jako jeden celek, kde fyzikální vrstva přímo definuje limity a možnosti digitální bezpečnosti. Kurz připravuje na reálné výzvy při nasazování kvantových technologií do stávající telekomunikační infrastruktury.

QNIE-QC1	Kvantové výpočty 1	Z,ZK	6

The course introduces the student to basic principles of quantum computation and shows the difference between classical and quantum mechanics. Quantum computation uses quantum circuits, which will be demonstrated in the Qiskit SDK. The course will gradually introduce the student to such concepts the state of a quantum system and its visualization, measurements, basic gates and their composition, and the so-called entanglement. The student will be introduced to the BB84 and E91 protocols as demonstrations of the properties of quantum states. The course will also cover quantum teleportation, quantum oracle queries, the Deutsch-Jozsa algorithm, the quantum Fourier transform, the phase estimation algorithm, and the Shor algorithm.

QNIE-QC2	Kvantové výpočty 2	Z,ZK	6

Quantum Computing 2 focuses on advanced quantum algorithms and their implementations: the Grover algorithm and its applications, quantum algorithms solving linear algebra problems, HHL for solving systems of linear equations. In the course we also introduce students to variational methods and error correction.

QNIE-LOM	Lineární optimalizace a metody	Z,ZK	5

Students will gain an overview of applications of optimization methods in computer science, economics and industrial practice. They will be introduced to the practical importance of linear and integer programming. They will be able to work with optimization software and to master the languages used in its programming. They will be able to formalise optimisation problems in the areas of computer science (e.g. task allocation to processors, network flow analysis), resource distribution and allocation (traffic problems, business traveller problem, etc.). Gain an overview of computational complexity issues in optimization. Gain a good understanding of linear programming algorithms and selected integer linear programming algorithms.

QNIE-MPR	Magisterský projekt	Z	7

1. Student si na začátku semestru vybere téma práce (viz Instrukce pro výběr tématu a jeho registraci). S vedoucím si domluví dílčí úkoly, které na zpracování zadání vykoná během semestru. Pokud tyto úkoly splní, udělí mu vedoucí práce na konci semestru zápočet z předmětu NI-MPR. 2. Externí vedoucí práce zadá informaci o udělení zápočtu pomocí formuláře Udělení zápočtu od externího vedoucího závěrečné práce (viz Ke stažení). Vyplněný a podepsaný formulář je potřeba doručit osobně nebo e-mailem referentce pro SZZ, která udělení zápočtu zařídí. 3. Je-li téma práce, které si student rezervoval, formulováno obecněji, měly by úkoly, které mu vedoucí na semestr uloží, směřovat primárně k doladění zadání tak, aby mohlo být zadání práce koncem semestru doplněno a schváleno. Domluva s vedoucím práce, týkající se upřesnění požadavků pro předmět NI-MPR by měla proběhnout v prvních týdnech semestru. Aktivita a odpovědnost leží na studentovi, nikoliv na vedoucím práce. Z hlediska splnění podmínek rozhodně nestačí, aby si student vybral téma. Může dojít k situaci, že se student na konci semestru rozhodne na tématu závěrečné práce dále nepracovat a zvolí si jiné. Stejně tak může vedoucí práce ukončit spolupráci se studentem. I v tomto případě je možné udělit zápočet.

QNIE-MQI	Matematika pro kvantovou informatiku	Z,ZK	6

Linear algebra on finite dimensional spaces with scalar product, Hilbert spaces, Dirac's bra-ket formalism, normal, Hermitian and unitary operators, operator spectrum, orthonormalization, diagonalization, matrix exponential, tensor product of vector spaces and operators. Discrete Fourier transform and fast Fourier transform.

QNIE-PPS	Programování paralelních systémů	Z,ZK	6

Nowadays, multi-core processors and GPU accelerators have become common components of computing clusters and high-performance computing systems, so knowledge and skills related to parallel programming are essential for every computer scientist. The aim of this course is to introduce students to the architectures and programming methods of parallel computers with shared memory, GPU accelerators, or with distributed memory. To effectively use these modern computing systems, it is essential to combine parallelization techniques at all three levels. Students will gain knowledge of the relevant programming models, languages and environments. They will become familiar with fundamental parallel algorithms and be able to analyze the limitations, efficiency, and scalability of parallel solutions to selected problems on high-performance computing systems. In addition to the necessary theory in lectures, students will gain practical experience and skills in programming in OpenMP, CUDA and MPI environments.

QNIE-TIN	Teorie informace	Z,ZK	6

The course focuses on the mathematical description of a random message source, its coding and transmission of the source through a noisy channel. The coding problem is addressed probabilistically, the relation of the mean length of the optimal code with the entropy and entropy rate of the random source is emphasized. In the case of the noisy channel we focus on the set of typical sequences and its appropriate coding by self-correcting codes. The course includes a reminder of necessary concepts such as conditional distributions, goodness-of-fit and independence tests, and an introduction to random chains.

QNIE-CPX	Teorie složitosti	Z,ZK	6

Students will learn about the fundamental classes of problems in the complexity theory and different models of algoritms and about implications of the theory concerning practical (in)tractability of difficult problems.

QNIE-UKT	Úvod do kvantové teorie	Z,ZK	6

interpretation of quantum theory are explained using simple models mainly from finite-dimensional quantum mechanics. Emphasis is placed on further applications of quantum theory to information processing and communication. Possible physical realizations of a qubit, description of multipartite systems, quantum entanglement and its applications are discussed. The course concludes with a description of continuous quantum systems in infinite-dimensional Hilbert spaces, in particular the linear harmonic oscillator as a description of the mode of a quantized electromagnetic field.

Název bloku: Povinně volitelné předměty
Minimální počet kreditů bloku: 24
Role bloku: PV

Kód skupiny: QNIE-PV
Název skupiny: Compulsory elective courses of the QNIE Quantum Informatics programme
Podmínka kredity skupiny: V této skupině musíte získat alespoň 24 kreditů (maximálně 68)
Podmínka předměty skupiny: V této skupině musíte absolvovat alespoň 4 předměty (maximálně 13)
Kredity skupiny: 24
Poznámka ke skupině: Beware of the knowledge prerequisite of the QNI-QML course. You can enroll only with the previous knowledge, which is discussed in the following bachelor's courses: BIE-ML1.21 Strojové učení 1 BIE-ML2.21 Strojové učení 2

Kód	Název předmětu / Název skupiny předmětů *(u skupiny předmětů seznam kódů jejích členů)* *Vyučující,* ***autoři*** *a garanti (gar.)*	Zakončení	Kredity	Rozsah	Semestr	Role
BQM36AVM	**Adiabatické a variační metody** *Jakub Mareček* ***Jakub Mareček*** *Jakub Mareček (Gar.)*	Z,ZK	6	2P+2C		PV
BQM36QTC	**Kvantová (stavová, procesní, kanálová) tomografie a kvantové optimální řízení** *Jakub Mareček* ***Jakub Mareček*** *Jakub Mareček (Gar.)*	Z,ZK	6	2P+2C		PV

BQM36KPB	**Kvantové počítání v bankovnictví** *Jakub Mareček* ***Jakub Mareček*** *Jakub Mareček (Gar.)*	Z,ZK	5	2P+2C		PV
QNIE-NMK	**Numerical methods for quantum computation**	Z,ZK	5	2P+2C		PV
QNIE-OQC	**Optical quantum computing**	Z,ZK	5	2P+1C	Z	PV
QNIE-OVV	**Optimization for Scientific Computing**	Z,ZK	5	2P+1C		PV
QNIE-PNM	**Parallelization of numerical methods**	Z,ZK	5	2P+2C		PV
QNIE-PJK	**Programming languages for quantum computing** *Jan Janoušek* ***Jan Janoušek*** *Jan Janoušek (Gar.)*	Z,ZK	5	2P+1C	L	PV
QNIE-QEC	**Quantum error correction**	Z,ZK	5	2P+2C	Z	PV
QNIE-QML	**Quantum machine learning**	Z,ZK	5	2P+1C	Z	PV
QNIE-QOM	**Quantum Optics, Metrology, Sensing and Imaging**	Z,ZK	5	2P+2C	Z	PV
QNIE-PON	**Selected Topics in Optimization and Numerical mathematics**	Z,ZK	5	2P+1C	L	PV

Charakteristiky předmětů této skupiny studijního plánu: Kód=QNIE-PV Název=Compulsory elective courses of the QNIE Quantum Informatics programme

BQM36AVM	Adiabatické a variační metody	Z,ZK	6
Kurz představuje adiabatické výpočty a variační kvantové algoritmy (VQA).			
BQM36QTC	Kvantová (stavová, procesní, kanálová) tomografie a kvantové optimální řízení	Z,ZK	6
Kurz představuje klíčové optimalizační problémy v návrhu a analýze kvantových systémů.			
BQM36KPB	Kvantové počítání v bankovnictví	Z,ZK	5
QNIE-NMK	Numerical methods for quantum computation	Z,ZK	5
The course is devoted to numerical solution of boundary-value problems and intial-boundary-value problems for ordinary and partial differential equations. It explains finite-difference, finite-element and finite-volume methods for elliptic, parabolic and hyperbolic partial differential equations. Students are introduced to the recent advances in methods solving the mentioned problems.			
QNIE-OQC	Optical quantum computing	Z,ZK	5
The course covers the basic theoretical methods and concepts for optical quantum computing, complemented by on hands-on exercise and applications using quantum programming libraries, Strawberry Fields and Piquasso. Theoretical concepts include measurement-based quantum computation, Gaussian Boson Sampling, and quantum supremacy. Applications feasible on current and near-term hardware include recent generative and discriminative machine-learning algorithms, as well as molecular vibration simulations.			
QNIE-OVV	Optimization for Scientific Computing	Z,ZK	5
The content of the course is an explanation of numerical methods for solving nonlinear optimization, convex optimization, stochastic optimization, optimal control, applications for QC, genetic and evolutionary programming, machine learning, deep neural networks. Students are also introduced to modern trends in solving these problems.			
QNIE-PNM	Parallelization of numerical methods	Z,ZK	5
The content of the course is an explanation of numerical methods for solving mathematical models with a focus on their parallelization and the use of these methods in QC. Students are also introduced to modern trends in the field of solving these problems.			
QNIE-PJK	Programming languages for quantum computing	Z,ZK	5
Computational models for quantum computing: quantum Turing machine, QRAM, lambda calculus with qubits. Higher programming languages for quantum computation: imperative languages (Silq), functional languages (QML, Quipper).). In the seminars the student will learn the basics of programming in the higher programming language Silq.			
QNIE-QEC	Quantum error correction	Z,ZK	5
In this course, we will build a theory for the construction of quantum error-correcting codes. In the introductory part, necessary chapters from the classical theory will be summarized, atop of which we then present the quantum analogy. We will show how coherently stored quantum information can be made robust to loss and noise. We conclude the course by arriving at the principle of fault tolerance, based on which quantum computers are able to continuously correct errors arising at runtime and thus achieve correct results even with erroneous bits, gates or measurements.			
QNIE-QML	Quantum machine learning	Z,ZK	5
The aim of the course is to introduce students to quantum machine learning. Students will first learn theoretically and practically about the quantum representation of classical data. Next, they will explore kernel methods, the quantum SVM model, and the use of quantum variational methods in supervised learning scenarios. The course will also introduce quantum neural networks and quantum generative adversarial models in unsupervised learning scenarios. The primary focus of the course is quantum algorithms for classical data. The exercises will use the pandas and qiskit libraries for Python to work with data and models.			
QNIE-QOM	Quantum Optics, Metrology, Sensing and Imaging	Z,ZK	5
Students are given an introduction to the quantum theory of light and related fundamental principles with an emphasis on practical aspects. They acquire the theoretical and experimental foundations for the development of specifically quantum mechanical approaches to metrology and imaging in quantum computing and communications. Specific problems discussed include elementary processes with photons (absorption, emission, stimulated emission), interference, entanglement, non-classical phenomena with photons, methods of suppressing optical aberrations and dispersion. The various techniques are explained theoretically and also using experiments that demonstrate these principles in practice.			
QNIE-PON	Selected Topics in Optimization and Numerical mathematics	Z,ZK	5
Students will be introduced to special optimization problems that arise in the field of machine learning and artificial intelligence and will extend the basic knowledge of continuous optimization acquired in previous studies. They will also learn about the details of implementing solutions to these problems on a computer and related mathematical concepts, especially from numerical linear algebra.			

Název bloku: Volitelné předměty
Minimální počet kreditů bloku: 0
Role bloku: V

Kód skupiny: QNIE-V
Název skupiny: Purely Elective Master's Courses in the academic programme Quantum Informatics
Podmínka kredity skupiny:
Podmínka předměty skupiny:
Kredity skupiny: 0

Poznámka ke skupině: In addition to the courses listed here, you can enroll as an elective any course that is offered within your study program and form of study that you did not enroll as a compulsory subject in the program/branch/specialization or a compulsory elective course.Courses of this group that a student has completed in the bachelor study at CTU cannot be re-completed.

Kód	Název předmětu / Název skupiny předmětů *(u skupiny předmětů seznam kódů jejích členů)* *Vyučující,* ***autoři*** *a garanti (gar.)*	Zakončení	Kredity	Rozsah	Semestr	Role
QNIE-AVM	**Adiabatic computing and variational methods**	Z,ZK	6	2P+2C	*	v
NIE-KRY	**Advanced Cryptology** *Róbert Lórencz, Jiří Buček* ***Jiří Buček*** *Róbert Lórencz (Gar.)*	Z,ZK	5	2P+2C	Z	v
NIE-AOS	**Advanced Operating Systems**	Z,ZK	5	2P+1C	Z	v
NIE-APT	**Advanced Program Testing** *Pierre Donat-Bouillud* ***Pierre Donat-Bouillud*** *Pierre Donat-Bouillud (Gar.)*	Z,ZK	5	2P+1C	Z	v
NIE-AIB	**Algorithms of Information Security** *Martin Jureček* ***Martin Jureček*** *Martin Jureček (Gar.)*	Z,ZK	5	2P+1C	Z	v
FIT-BIP	**Blended Intensive Programme** ***Zdeněk Muzikář*** *Zdeněk Muzikář (Gar.)*	Z	3		Z,L	v
NIE-BLO	**Blockchain** *Josef Gattermayer, Marek Bielik, Jakub Růžička* ***Josef Gattermayer*** *Josef Gattermayer (Gar.)*	Z,ZK	5	1P+2C	Z	v
NIE-GEN	**Code Generators** *Petr Máj* ***Petr Máj*** *Jan Janoušek (Gar.)*	Z,ZK	5	2P+1C	Z	v
NIE-CPX.26	**Complexity Theory** ***Dušan Knop***	Z,ZK	6	3P+1C	Z	v
NIE-KOD	**Data Compression** *Jan Holub* ***Jan Holub*** *Jan Holub (Gar.)*	Z,ZK	5	2P+1C	L	v
NIE-DSS	**Decision Support Systems** *Robert Pergl, Petra Pavlíčková* ***Petra Pavlíčková*** *Robert Pergl (Gar.)*	Z,ZK	5	2P+1C	Z	v
FITE-DIF	**Differential equations** *Ondřej Bouchala, Antonella Marchesiello, Jan Valdman Ondřej Bouchala (Gar.)*	Z,ZK	5	2P+2C	L	v
ANIE-SIM	**Digital Circuit Simulation and Verification**	Z,ZK	5	2P+1C	Z	v
NIE-DSV	**Distributed Systems and Computing** *Pavel Tvrdík, Peter Macejko* ***Pavel Tvrdík*** *Pavel Tvrdík (Gar.)*	Z,ZK	5	2P+1C	Z	v
NIE-EPC	**Effective C++ programming** *Daniel Langr* ***Daniel Langr*** *Daniel Langr (Gar.)*	Z,ZK	5	2P+1C	Z	v
NIE-EVY	**Efficient Text Pattern Matching** *Jan Holub* ***Jan Holub*** *Jan Holub (Gar.)*	Z,ZK	5	2P+1C	Z	v
ANIE-EHW	**Embedded hardware**	Z,ZK	5	2P+2C	L	v
ANIE-BVS	**Embedded Security**	Z,ZK	5	2P+2C	L	v
ANIE-ESW	**Embedded software**	Z,ZK	5	2P+2C	Z	v
ANIE-BKO	**Error Control Coding**	Z,ZK	5	2P+1C	L	v
NIE-GPU	**GPU Architectures and Programming** *Ivan Šimeček* ***Ivan Šimeček*** *Ivan Šimeček (Gar.)*	Z,ZK	5	2P+1C	L	v
NIE-GAK.26	**Graph theory and combinatorics**	Z,ZK	6	2P+2C	L	v
NIE-HWB	**Hardware Security** *Jiří Buček* ***Jiří Buček*** *Jiří Buček (Gar.)*	Z,ZK	5	2P+2C	L	v
FITE-EHD	**Introduction to European Economic History** *Tomáš Evan* ***Tomáš Evan*** *Tomáš Evan (Gar.)*	Z,ZK	3	2P+1C	L	v
NIE-LOM	**Linear Optimization and Methods** *Dušan Knop* ***Dušan Knop*** *Dušan Knop (Gar.)*	Z,ZK	5	2P+0S+1C	Z	v
ANIE-MLM	**Machine Learning Methods**	Z,ZK	5	2P+1C		v
NIE-MKY.26	**Mathematics for Cryptology** ***Róbert Lórencz***	Z,ZK	7	3P+2C	L	v
NIE-MPS	**Modern Computer Networks** ***Jan Fesl***	Z,ZK	5	2P+2C	Z	v
NIE-MCC	**Multicore CPU Computing** *Daniel Langr, Ivan Šimeček* ***Ivan Šimeček*** *Ivan Šimeček (Gar.)*	Z,ZK	5	2P+1C	Z	v
ANIE-COM	**Network Communication** *Tomáš Čejka* ***Tomáš Čejka*** *Tomáš Čejka (Gar.)*	Z,ZK	5	2P+1C		v
NIE-SIB	**Network Security** *Simona Fornůsek, Jiří Dostál, Tomáš Zahradnický, Gramoz Cubreli* ***Simona Fornůsek*** *Simona Fornůsek (Gar.)*	Z,ZK	5	2P+1C	L	v
QNIE-NMK	**Numerical methods for quantum computation**	Z,ZK	5	2P+2C		v
QNIE-OPM	**Optical measurements**	Z,ZK	6	2P+2C		v
QNIE-OQC	**Optical quantum computing**	Z,ZK	5	2P+1C	Z	v
QNIE-OVV	**Optimization for Scientific Computing**	Z,ZK	5	2P+1C		v
QNIE-PNM	**Parallelization of numerical methods**	Z,ZK	5	2P+2C		v
NIE-PAM	**Parameterized Algorithms** *Ondřej Suchý* ***Ondřej Suchý*** *Ondřej Suchý (Gar.)*	Z,ZK	4	2P+1C	L	v

NIE-SYP	**Parsing and Compilers** *Jan Janoušek **Jan Janoušek** Jan Janoušek (Gar.)*	Z,ZK	5	2P+1C	Z	v
NIE-PML	**Personalized Machine Learning** *Rodrigo Augusto Da Silva Alves **Karel Klouda** Rodrigo Augusto Da Silva Alves (Gar.)*	Z,ZK	5	2P+1C	Z	v
NIE-PDL	**Practical Deep Learning** *Martin Barus, Yauhen Babakhin **Karel Klouda** Karel Klouda (Gar.)*	KZ	5	2P+1C	Z	v
QNIE-PJK	**Programming languages for quantum computing** *Jan Janoušek **Jan Janoušek** Jan Janoušek (Gar.)*	Z,ZK	5	2P+1C	L	v
FIT-PMA	**Programování v Mathematica** *Zdeněk Buk **Zdeněk Buk** Zdeněk Buk (Gar.)*	Z,ZK	4	2P+2C	Z,L	v
QNIE-QEC	**Quantum error correction**	Z,ZK	5	2P+2C	Z	v
QNIE-QML	**Quantum machine learning**	Z,ZK	5	2P+1C	Z	v
QNIE-KOS	**Quantum Optical Communications and Networks**	Z,ZK	6	2P+2C		v
QNIE-QOM	**Quantum Optics, Metrology, Sensing and Imaging**	Z,ZK	5	2P+2C	Z	v
NIE-REV	**Reverse Engineering** *Josef Kokeš **Josef Kokeš** Josef Kokeš (Gar.)*	Z,ZK	5	1P+2C	Z	v
NIE-RUN	**Runtime systémy** *Filip Křikava, Filip Říha **Filip Křikava** Filip Křikava (Gar.)*	Z,ZK	5	2P+1C	L	v
NIE-APR	**Selected Methods for Program Analysis** ***Filip Křikava***	Z,ZK	5	2P+1C	Z	v
QNIE-PON	**Selected Topics in Optimization and Numerical mathematics**	Z,ZK	5	2P+1C	L	v
NIE-SEM	**Semantics of Programming Languages**	Z,ZK	5	2P+1C	Z	v
NIE-SBF	**System Security and Forensics** *Jiří Buček, Simona Fornůsek, Tomáš Zahradnický, Marián Svetlík **Simona Fornůsek** Simona Fornůsek (Gar.)*	Z,ZK	5	2P+1C	Z	v
ANIE-TSP	**Testing and Reliability**	Z,ZK	5	2P+2C	Z	v
NIE-VCC	**Virtualization and Cloud Computing** *Tomáš Vondra **Tomáš Vondra** Tomáš Vondra (Gar.)*	Z,ZK	5	2P+1C	L	v
FITE-SEP	**World Economy and Business** *Tomáš Evan **Tomáš Evan** Tomáš Evan (Gar.)*	Z,ZK	4	2P+2C	Z	v

Charakteristiky předmětů této skupiny studijního plánu: Kód=QNIE-V Název=Purely Elective Master's Courses in the academic programme Quantum Informatics

QNIE-NMK	Numerical methods for quantum computation	Z,ZK	5

The course is devoted to numerical solution of boundary-value problems and intial-boundary-value problems for ordinary and partial differential equations. It explains finite-difference, finite-element and finite-volume methods for elliptic, parabolic and hyperbolic partial differential equations. Students are introduced to the recent advances in methods solving the mentioned problems.

QNIE-OQC	Optical quantum computing	Z,ZK	5

The course covers the basic theoretical methods and concepts for optical quantum computing, complemented by on hands-on exercise and applications using quantum programming libraries, Strawberry Fields and Piquasso. Theoretical concepts include measurement-based quantum computation, Gaussian Boson Sampling, and quantum supremacy. Applications feasible on current and near-term hardware include recent generative and discriminative machine-learning algorithms, as well as molecular vibration simulations.

QNIE-OVV	Optimization for Scientific Computing	Z,ZK	5

The content of the course is an explanation of numerical methods for solving nonlinear optimization, convex optimization, stochastic optimization, optimal control, applications for QC, genetic and evolutionary programming, machine learning, deep neural networks. Students are also introduced to modern trends in solving these problems.

QNIE-PNM	Parallelization of numerical methods	Z,ZK	5

The content of the course is an explanation of numerical methods for solving mathematical models with a focus on their parallelization and the use of these methods in QC. Students are also introduced to modern trends in the field of solving these problems.

QNIE-PJK	Programming languages for quantum computing	Z,ZK	5

Computational models for quantum computing: quantum Turing machine, QRAM, lambda calculus with qubits. Higher programming languages for quantum computation: imperative languages (Silq), functional languages (QML, Quipper).). In the seminars the student will learn the basics of programming in the higher programming language Silq.

QNIE-QEC	Quantum error correction	Z,ZK	5

In this course, we will build a theory for the construction of quantum error-correcting codes. In the introductory part, necessary chapters from the classical theory will be summarized, atop of which we then present the quantum analogy. We will show how coherently stored quantum information can be made robust to loss and noise. We conclude the course by arriving at the principle of fault tolerance, based on which quantum computers are able to continuously correct errors arising at runtime and thus achieve correct results even with erroneous bits, gates or measurements.

QNIE-QML	Quantum machine learning	Z,ZK	5

The aim of the course is to introduce students to quantum machine learning. Students will first learn theoretically and practically about the quantum representation of classical data. Next, they will explore kernel methods, the quantum SVM model, and the use of quantum variational methods in supervised learning scenarios. The course will also introduce quantum neural networks and quantum generative adversarial models in unsupervised learning scenarios. The primary focus of the course is quantum algorithms for classical data. The exercises will use the pandas and qiskit libraries for Python to work with data and models.

QNIE-QOM	Quantum Optics, Metrology, Sensing and Imaging	Z,ZK	5

Students are given an introduction to the quantum theory of light and related fundamental principles with an emphasis on practical aspects. They acquire the theoretical and experimental foundations for the development of specifically quantum mechanical approaches to metrology and imaging in quantum computing and communications. Specific problems discussed include elementary processes with photons (absorption, emission, stimulated emission), interference, entanglement, non-classical phenomena with photons, methods of suppressing optical aberrations and dispersion. The various techniques are explained theoretically and also using experiments that demonstrate these principles in practice.

QNIE-PON	Selected Topics in Optimization and Numerical mathematics	Z,ZK	5

Students will be introduced to special optimization problems that arise in the field of machine learning and artificial intelligence and will extend the basic knowledge of continuous optimization acquired in previous studies. They will also learn about the details of implementing solutions to these problems on a computer and related mathematical concepts, especially from numerical linear algebra.

QNIE-AVM	Adiabatic computing and variational methods	Z,ZK	6
The course introduces adiabatic computing and variational quantum algorithms (VQA). We start with a broad introduction to variational methods in physical chemistry (e.g., for calculating ground state of small molecules) and a recapitulation of advances in theoretical computer science (computational complexity and problems such as MAXCUT). We will present the EQA Conjecture and the unique games conjecture. We will present the adiabatic theorem and quantum speedup by quantum annealing (QA). We will build up an understanding of variational quantum algorithms by introducing and analysing, in turn, Variational quantum eigensolver (VQE), Quantum Approximate Optimization Algorithm (QAOA), and their Warm-started variants. As applications, we will highlight variational solvers for systems of linear equations and variational solvers for Markowitz portfolio management, with some discussion of the challenges in benchmarking of VQA.			
NIE-KRY	Advanced Cryptology	Z,ZK	5
Students will learn the essentials of cryptanalysis and the mathematical principles of constructing symmetric and asymmetric ciphers. They will know the mathematical principles of random number generators. They will have an overview of cryptanalysis methods, elliptic curve cryptography and quantum cryptography, which they can apply to the integration of their own systems or to the creation of their own software solutions.			
NIE-AOS	Advanced Operating Systems	Z,ZK	5
Předmět se zabývá problematikou systémového programování v operačních systémech unixového typu se zaměřením na vývoj jádra OS a pokročilými technologiemi pro správu unixových operačních systémů. Studenti se seznámí s architekturou a datovými strukturami jádra OS, se správou procesů a hlavní paměti, s vnitřní architekturou moderních systémů souborů, s implementacemi metod ovládání periferních zařízení a síťové komunikace, s metodami bootování jádra i vlastního operačního systému a s technikami ladění jádra pomocí dynamické instrumentace. Dále získají znalosti o postupech při vývoji a modifikacích jádra OS a zajištění přenositelnosti jádra a o využívání technologií kontejnerizace a virtualizace. Studenti se seznámí se specifikami implementace jádra OS pro vestavné systémy či pro systémy reálného času. Teoretické a obecné principy budou demonstrovány primárně na jádru Linuxu. Cvičení budou zaměřena na vývoj modulů jádra Linuxu a na nástroje pro správu probraných technologií.			
NIE-APT	Advanced Program Testing	Z,ZK	5
Testing a program is essential to ensure that a program respects its specification, that changes do not introduce regressions or security issues. The goal of the course is to present advanced program testing techniques, beyond writing unit tests, especially fuzzing and symbolic execution.			
NIE-AIB	Algorithms of Information Security	Z,ZK	5
Studenti se seznámí s algoritmy bezpečného generování klíčů a kryptografickým zpracováním chybových (nejen biometrických) dat. Dále se studenti seznámí s matematickými principy kryptografických protokolů (identifikačních, autentizačních a podpisových schémat). Získají znalosti o metodách detekce malware a použití strojového učení v detekčních algoritmech. Taktéž se seznámí s metodami vytváření steganografických záznamů, s metodami pro jejich vyhledávání a s útoky na ně.			
FIT-BIP	Blended Intensive Programme	Z	3
Blended Intensive Program: krátkodobý výjezd přes program Erasmus+			
NIE-BLO	Blockchain	Z,ZK	5
Students will understand the foundations of blockchain technology, smart contract programming, and gain an overview of most notable blockchain platforms. They will be able to design, code and deploy a secure decentralized application, and assess whether integration of a blockchain is suitable for a given problem. The course places an increased emphasis on the relationship between blockchains and information security. It is concluded with a defense of a research or applied semester project, which prepares the students for implementing or supervising implementation of blockchain-based solutions in both academia and business.			
NIE-GEN	Code Generators	Z,ZK	5
Advanced techniques of translating programs written in high-level programming languages are essential for understanding the field of systems programming. This primarily involves understanding the algorithms and techniques used to translate more complex programming constructs of modern languages employed in systems programming. Students will become familiar with both the theoretical and practical aspects of implementing the back-end of optimizing compilers for programming languages.			
NIE-CPX.26	Complexity Theory	Z,ZK	6
Studenti se dozvědí o základních třídách teorie výpočetní složitosti a různých modelech algoritmů a o implikacích této teorie týkajících se praktické algoritmické (ne)řešitelnosti složitých úloh.			
NIE-KOD	Data Compression	Z,ZK	5
Students are introduced to the basic principles of data compression. They will learn the necessary theoretical background and get an overview of data compression methods being used in practice. The overview covers principles of integer coding and of statistical, dictionary, and context data compression methods. In addition, students learn the fundamentals of lossy data compression methods used in image, audio, and video compression.			
NIE-DSS	Decision Support Systems	Z,ZK	5
The aim of the course is to provide students with knowledge and skills in decision support systems, their classification (Powerova), selected principles of data-oriented, model-oriented and knowledge-oriented decision support systems. Students will also gain knowledge of multicriterial decision-making methods and game theory. They will also learn about the principles of conceptually and ontologically oriented decision support systems and the basics of distribution, optimization and evolution methods and algorithms.			
FITE-DIF	Differential equations	Z,ZK	5
This course provides a foundational overview of differential equations, starting with basic motivation and examples of ODEs and progressing to essential solution methods like separation of variables. Key theorems on existence and uniqueness establish when solutions can be guaranteed. Linear and system-based ODEs are covered with methods like characteristic polynomial analysis, followed by examples of non-linear models such as predator-prey and epidemiological models to showcase real-world applications. Finally, an introduction to partial differential equations (PDEs) extends these concepts to multi-variable contexts. The course will also cover numerical methods for solving ODEs and PDEs, including implicit and explicit Euler methods, Runge-Kutta methods, and finite element methods for both ODEs and PDEs.			
ANIE-SIM	Digital Circuit Simulation and Verification	Z,ZK	5
Studenti získají podrobné informace o principech kvaziparalelní simulace číslicových obvodů na úrovni RTL (Register Transfer Level) i TLM (Transaction Level Modeling) a o vlastnostech pro tyto účely aktuálně používaných nástrojů. Předmět pokrývá i současné možnosti verifikace, zejména s použitím metodologie UVM (Universal Verification Methodology).			
NIE-DSV	Distributed Systems and Computing	Z,ZK	5
Students are introduced to methods for coordination of processes in distributed environment characterised by nondeterministic time responses of computing processes and communication channels. They learn basic algorithms that assure correctness of computations realized by a group of loosely coupled processes and mechanisms that support high availability of both data and services, and safety in case of failures.			
NIE-EPC	Effective C++ programming	Z,ZK	5
Students learn how to use the modern features of contemporary versions of the C++ programming language for software development. The course focuses on programming effectivity and efficiency in the form of writing maintainable and portable source code and creating correct programs with low memory and processor time requirements.			
NIE-EVY	Efficient Text Pattern Matching	Z,ZK	5
Students get knowledge of efficient algorithms for text pattern matching. They learn to use so called succinct data structures that are efficient in both access time and memory complexity. They will be able to use the knowledge in design of applications that utilize pattern matching.			
ANIE-EHW	Embedded hardware	Z,ZK	5
Předmět poskytuje znalost základních technik a zákonitostí, které řídí konstrukci číslicových zařízení jak malého, tak velkého měřítka. Jsou základem konstrukce pokročilých vestavných systémů, které využívají specializaci své funkce ke konstrukci efektivní hardwarové realizace či podpory výpočtu. Probírají se techniky konstrukce rychlých systémů, jejich standardní vnitřní komunikace, využití přirozeného paralelismu výpočtu ve specializovaných strukturách a systémových architekturách.			

ANIE-BVS	Embedded Security	Z,ZK	5
Studenti získají základní znalosti ve vybraných kapitolách z kryptografie a kryptoanalýzy se zaměřením na vestavné systémy. Důraz je tedy kladen na efektivní implementace kryptografických primitiv v hardwaru a ve firmwaru, což si studenti ověří na konkrétních laboratorních úlohách. Předmětem je jak symetrická kryptografie (šifry s jedním společným klíčem), tak asymetrická kryptografie (RSA, Kryptografie Eliptických křivek, Diffie-Hellmanova výměna klíčů nad EC). Předmět se dále soustřeďuje na vybrané útoky na kryptografické systémy implementované ve vestavných zařízeních. Studenti tak získají vědomosti o některých potenciálních rizicích kryptografických systémů a budou lépe schopni jim čelit.			
ANIE-ESW	Embedded software	Z,ZK	5
Předmět seznamuje studenty se specifiky vývoje programového vybavení pro vestavné systémy. Předmět studenta provází od základních technik programování v jazyce C a optimalizace kódu, přes řadu typických oblastí, jako je vývoj spolehlivého programového vybavení, vestavné operační systémy či zpracování signálu, až po sofistikované techniky vývoje vestavného programového vybavení kombinované s umělou inteligencí.			
ANIE-BKO	Error Control Coding	Z,ZK	5
Předmět rozšiřuje základní znalosti o bezpečnostních kódech používaných v současných systémech pro detekci a opravu chyb. Podává potřebnou matematické teorii a principy lineárních, cyklických kódů a kódů pro opravu násobných chyb, shluků chyb i celých slabik (bytů). Studenti se také dozvědí, jak tyto detekce a opravy implementovat pro různé typy přenosů (paralelní, sériové) při ukládání dat do pamětí a při přenosu telekomunikačními kanály.			
NIE-GPU	GPU Architectures and Programming	Z,ZK	5
Students will gain knowledge of the internal architecture of modern massively parallel GPU processors. They will learn to program them mainly in the CUDA programming environment, which is already a widespread programming technology of GPU processors. As an integral part of the effective computational use of these hierarchical computational structures, students will also learn optimization programming techniques and methods of programming multiprocessor GPU systems.			
NIE-GAK.26	Graph theory and combinatorics	Z,ZK	6
Předmět si klade za cíl seznámit studenta s nejdůležitějšími partiemi teorie grafů, kombinatorických principů a struktur, diskrétních modelů a algoritmů. Kromě pochopení teoretických principů bude kladen důraz i na aplikaci poznatků při řešení úloh a navrhování algoritmů. Mezi probíraná témata patří technika generujících funkcí, vybrané partie z barevnosti grafů a hypergrafů, Ramseyovské věty, úvod do pravděpodobnostních technik a studium vlastností různých speciálních tříd grafů a kombinatorických struktur.			
NIE-HWB	Hardware Security	Z,ZK	5
The course provides the knowledge needed for the analysis and design of computer systems security solutions. Students get an overview of safeguards against abuse of the system using hardware means. They will be able to safely use and integrate hardware components into systems and test them for resistance to attacks. Students will gain knowledge about the cryptographic accelerators, PUF, random number generators, smart cards, biometric devices, and devices for internal security functions of the computer.			
FITE-EHD	Introduction to European Economic History	Z,ZK	3
The course introduces a selection of themes from European economic history. It gives the student basic knowledge about forming of the global economy through the description of the key historical periods. As European countries have been dominant actors in this process it focuses predominantly on their roles in economic history. From the large economic area of the Roman Empire to the fragmentation of the Middle Ages, from the destruction of WWII to the current affairs, the development of modern financial institutions is deciphered. The course does not cover the detailed economic history of particular European countries but rather the impact of trade and the role of particular events, institutions and organizations in history. Class meetings will consist of a mixture of lectures and discussions.			
NIE-LOM	Linear Optimization and Methods	Z,ZK	5
Students will gain an overview of applications of optimization methods in computer science, economics and industrial practice. They will be introduced to the practical importance of linear and integer programming. They will be able to work with optimization software and to master the languages used in its programming. They will be able to formalise optimisation problems in the areas of computer science (e.g. task allocation to processors, network flow analysis), resource distribution and allocation (traffic problems, business traveller problem, etc.). Gain an overview of computational complexity issues in optimization. Gain a good understanding of linear programming algorithms and selected integer linear programming algorithms.			
ANIE-MLM	Machine Learning Methods	Z,ZK	5
Předmět seznamuje studenty s metodami strojového učení, které uplatní ve svých specializacích navazujícího programu Aplikovaná informatika. Tyto principy a znalosti nejsou obsaženy ve společném bakářském profilu uchazečů, vyučují se jen ve specializacích zaměřených na umělou inteligenci. Cílem je porozumět teoretickým principům a naučit se prakticky používat modely vhodné pro regresní i klasifikační úlohy ve scénáři učení s učitelem včetně jádrových metod a neuronových sítí. Ve scénáři učení bez učitele se studenti seznámí zejména s modely shlukování a s analýzou hlavních komponent. V předmětu bude také probrána problematika vyhodnocování kvality modelů a základní techniky předzpracování dat. Na cvičeních se k práci s daty a modely budou využívat knihovny pandas, scikit a pytorch pro jazyk Python.			
NIE-MKY.26	Mathematics for Cryptology	Z,ZK	7
Studenti získají hlubší znalosti o algebraických postupech řešících nejdůležitější matematické problémy, na kterých je založena bezpečnost šifer. Zejména se jedná o problém řešení soustavy polynomiálních rovnic nad konečným tělesem, problém faktorizace velkých čísel a problém diskrétního logaritmu. Problém faktorizace bude speciálně řešen i na eliptických křivkách. Studenti se rovněž seznámí s moderními šifrovacími systémy založenými na počítání na mřížce.			
NIE-MPS	Modern Computer Networks	Z,ZK	5
Předmět je rozdělen na dvě komplementární části -- moderní síťové technologie a bezpečnost počítačových sítí. První část je věnována popisu principů moderních síťových technologií a komunikačních protokolů, které umožňují dosahovat vysokou propustnost, nízkou latenci a odolnost vůči chybám. Přednášky zahrnují i principy moderních softwarově definovaných sítí, které postupně nahrazují sítě klasické. První část je završena výkladem protokolů a technologií určených pro přenos videa a hlasu v reálném čase. V druhé části jsou nejprve představeny základní principy a technologie podporující a zvyšující bezpečnost počítačových sítí. Následné přednášky jsou věnovány vysvětlení principů známých síťových útoků v lokálních počítačových sítích a v Internetu. Na závěr jsou představeny moderní systémy umožňující detekci a eliminaci síťových útoků, včetně systémů pro sdílení informací umožňujících preventivně síťovým útokům předcházet. Studenti získají praktické zkušenosti s těmito koncepty v síťové laboratoři.			
NIE-MCC	Multicore CPU Computing	Z,ZK	5
Students will get acquainted in detail with hardware support and programming technologies for the creation of parallel multithreaded computations on multicore processors with shared and virtually shared memory, which are today the most common computing nodes of powerful computer systems. Students will gain knowledge of architecturally specific optimization techniques used to reduce the decrease in computing power due to the widening performance gap between the computational requirements of multi-core CPUs and memory interface throughput. On specific non-trivial multithreaded programs, students will also learn the basics of the art of creating these applications.			
ANIE-COM	Network Communication	Z,ZK	5
Předmět se zaměří na technické aspekty komunikace mezi zařízeními a systémy. V průběhu semestru budou přednášena témata od fyzických vrstev a komunikačních médií až po komunikační protokoly a monitorování provozu. Absolvent předmětu získá přehled o technických omezeních a možnostech komunikačních prostředků, které může využít při návrhu a vývoji reálných hardwarových nebo softwarových systémů.			
NIE-SIB	Network Security	Z,ZK	5
The students will gain theoretical and practical knowledge and experience in the area of current security threats in computer networks, specifically about detection and defense. The course explains basic pricipals of security monitoring, packet-based and flow-based analysis, in order to detect anomalies and suspicious network traffic. The course focuses on explanation and practical examples of various mechanisms of securing network infrastructure and detection in real time. The course covers general principals of handling detected security events (i.e. incident handling and incident response).			
QNIE-OPM	Optical measurements	Z,ZK	6
The aim of this course is to acquaint students with optical measurement methods from the detection of microparticles, non-regulation and surface breaches, through the use of fiber optics in areas where it is not possible to use standard electronic sensors, or in places with increased risk of explosion and in hospitals, lidars used in intelligent transport infrastructures, to macroscopic sensing (remote sensing) of the Earth, atmosphere and space. The inclusion of these measurement methods requires in particular an understanding of the physical mechanisms on which they are based, as well as knowledge of measurement procedures and specifics in data processing and reconstruction.			

NIE-PAM	Parameterized Algorithms	Z,ZK	4

There are many optimization problems for which no polynomial time algorithms are known (e.g. NP-complete problems). Despite that it is often necessary to solve these problems exactly in practice. We will demonstrate that many problems can be solved much more effectively than by naively trying all possible solutions. Often one can find a common property (parameter) of the inputs from practice-e.g., all solutions are relatively small. Parameterized algorithms exploit that by limiting the time complexity exponentially in this (small) parameter and polynomially in the input size (which can be huge). Parameterized algorithms also represent a way to formalize the notion of effective polynomial time preprocessing of the input, which is not possible in the classical complexity. Such a polynomial time preprocessing is then a suitable first step, whatever is the subsequent solution method. We will present a plethora of parameterized algorithm design methods and we will also show how to prove that for some problem (and parameter) such an algorithm (presumably) does not exist. We will also not miss out the relations to other approaches to hard problems such as moderately exponential algorithms or approximation schemes.

NIE-SYP	Parsing and Compilers	Z,ZK	5

The module builds upon the knowledge of fundamentals of automata theory, formal language and formal translation theories. Students gain knowledge of various variants and applications of LR parsing and are introduced to special applications of parsers, such as incremental and parallel parsing.

NIE-PML	Personalized Machine Learning	Z,ZK	5

Personalized machine learning (PML) is a sub-field of machine learning that aims to create models and predictions based on the unique characteristics and behaviors of individual entities. While PML is commonly used in applications such as recommender systems, which recommend items to users based on their personal interests, its principles can be applied to a wide range of other fields, including education, medicine, and chemical engineering. In this course, we will explore the latest PML methods from theoretical, algorithmic, and practical perspectives. Specifically, we will focus on cutting-edge models that are of interest to both the research and commercial communities.

NIE-PDL	Practical Deep Learning	KZ	5

This course is designed to provide students with a comprehensive understanding of Deep Learning using PyTorch, a popular open-source machine learning framework. Throughout the course, students will develop practical skills in building and training deep neural networks, using PyTorch to solve real-world problems in fields such as computer vision and natural language processing.

FIT-PMA	Programování v Mathematica	Z,ZK	4

Systém Wolfram Mathematica patří k nejvýkonnějším nástrojům pro vědecké a technické výpočty, analýzu dat a tvorbu interaktivních modelů. V jednom prostředí spojuje programování, matematiku, vizualizaci, automatizaci i reportování. Je využíván ve výzkumu, průmyslu i technologických společnostech po celém světě od inženýrů v NASA přes analytiky ve fintechu až po datové týmy ve farmaceutickém a automobilovém vývoji. Kurz FIT-PMA studenty provede od základů používání systému Mathematica až k samostatnému řešení složitějších úloh. Naučíte se efektivně kombinovat symbolické a numerické výpočty, psát přehledný a znovupoužitelný kód, pracovat s daty, vytvářet vizualizace a interaktivní dokumenty, automatizovat opakované úlohy a využívat pokročilé výpočetní metody a optimalizace. Důraz je kladen na praktické porozumění principům jazyka Wolfram Language jazyka, který je dnes jedním z nejuniverzálnějších nástrojů pro matematické modelování, datovou analýzu a algoritmický výzkum. Absolventi získají dovednosti využitelné v oblasti vědeckého a technického výzkumu, datové analýzy, softwarového vývoje i výuky matematiky a informatiky. Mathematica je běžně používána v akademických institucích i průmyslu jako prostředí pro rychlou tvorbu prototypů, experimentů a simulací.

QNIE-KOS	Quantum Optical Communications and Networks	Z,ZK	6

The course focuses on the basic principles and technologies for building and using quantum networks. Students will learn about the key components of quantum networks, including quantum repeaters, routers and switches, and their role in creating a scalable quantum Internet. Emphasis will be placed on quantum cryptography systems. Students will also learn the fundamentals of optics, optical networks, and classical cryptography as they relate to quantum key distribution (QKD) and quantum networks. The course will cover types and architectures of QKD systems (including practical implementation of quantum protocols) according to international standards, key generation and distribution in these systems, and integration of QKD with classical communication systems. Students will also have the opportunity to explore satellite and FSO QKD systems and integrated quantum photonics and electronics.

NIE-REV	Reverse Engineering	Z,ZK	5

Students will learn fundamentals of reverse engineering of computer software (methods of executing and initializing programs, organization of executable files, work with third-party libraries). Special attention will be paid to C ++. Students will also become familiar with the principles of debugging tools, disassemblers and obfuscation methods. Finally, the course will focus on code compression and decompression and executable file reconstruction.

NIE-RUN	Runtime systémy	Z,ZK	5

As the abstraction level of programming languages steadily rises, modern programs require greater and greater support during their runtime. This course introduces students to various aspects of the runtime support, such as runtime-effective program description, memory management support and garbage collection, just-in-time compilation, and interoperability with other languages and systems.

NIE-APR	Selected Methods for Program Analysis	Z,ZK	5

Tento kurz vás seznámí s programovou analýzou, tedy automatizovaným usuzováním o chování počítačového programu. Budeme se zabývat statickou i dynamickou analýzou. Ve statické analýze se podíváme na umění usuzování o programech bez jejich spuštění. Zaměříme se na analýzy pro porozumění programům, optimalizace a detekci chyb. V dynamické analýze se budeme zabývat analýzami, které zohledňují jednotlivé běhy programu v konkrétním prostředí a s konkrétními vstupy.

NIE-SEM	Semantics of Programming Languages	Z,ZK	5

Cílem předmětu je uvést studenty do základů sémantiky programovacích jazyků, která je základem pro studium a implementaci programovacích jazyků. Tyto techniky jsou také důležité pro verifikaci programů, implementaci optimalizací a obecný návrh programovacích jazyků. Důraz bude na porovnání operační a denotační sémantiky. Použité techniky mají uplatnění i v případě analýzy jazyků daných pouze pomocí operační sémantiky. Kurz umožní studentům získat potřebné dovednosti pro implementaci jazykových konstrukcí, ať už jejich popis pochází z teoretických nebo inženýrských zdrojů v literatuře.

NIE-SBF	System Security and Forensics	Z,ZK	5

Students will be introduced to various aspects of system security (principles of endpoint security, principles of security policies, security models, authentication concepts). Students will also learn about forensic analysis as a tool for investigating security incidents (techniques used by malicious software or attackers, forensic analysis techniques, and the importance of memory or file system artifacts for attack analysis and detection).

ANIE-TSP	Testing and Reliability	Z,ZK	5

Studenti získají přehled v oblasti testování číslicových obvodů a o metodách pro zvýšení spolehlivosti a bezpečnosti. Studenti budou schopni vytvořit test obvodu metodou intuitivního zcitlivění cesty, použít automatický generátor testovacích vzorků, budou schopni navrhnout snadno testovatelný obvod a obvod s vestavěným testovacím vybavením. Dále budou schopni analyzovat spolehlivost a provozuschopnost obvodů a aktivně ovlivňovat tyto parametry. Studenti budou schopni navržené znalosti využít v komplexních projektech návrhu obvodů ASIC i FPGA.

NIE-VCC	Virtualization and Cloud Computing	Z,ZK	5

Students will gain knowledge of architectures of large computer systems that are used in data centers and computer infrastructure of companies and organizations. They will get acquainted with virtualization principles, tools and technologies that serve to facilitate and automate configuration, testing and monitoring, and to efficiently operate and optimize the performance parameters of modern computer systems. Theoretically and practically, they will get acquainted with containerization as the most effective technology today for the management of complex computer systems and with specific technologies of cloud systems. Finally, they will learn the principles and gain practical skills in the use of modern integration and development tools (Continuous integration and development).

FITE-SEP	World Economy and Business	Z,ZK	4

The course introduces students of technical universities to international business. It does that predominantly by comparing individual countries and key regions of the world economy. Students get to know about different religions and cultures, necessary for doing business in diverse societies as well as indexes of economic freedom, corruption and economic development, which are needed for the right investment decision. Seminars help to improve knowledge in the form of discussions based on individual readings.

Seznam předmětů tohoto průchodu:

Kód	Název předmětu	Zakončení	Kredity
ANIE-BKO	Error Control Coding	Z,ZK	5
Předmět rozšiřuje základní znalosti o bezpečnostních kódech používaných v současných systémech pro detekci a opravu chyb. Podává potřebnou matematické teorii a principy lineárních, cyklických kódů a kódů pro opravu násobných chyb, shluků chyb i celých slabik (bytů). Studenti se také dozvědí, jak tyto detekce a opravy implementovat pro různé typy přenosů (paralelní, sériové) při ukládání dat do pamětí a při přenosu telekomunikačními kanály.			
ANIE-BVS	Embedded Security	Z,ZK	5
Studenti získají základní znalosti ve vybraných kapitolách z kryptografie a kryptoanalýzy se zaměřením na vestavné systémy. Důraz je tedy kladen na efektivní implementace kryptografických primitiv v hardwaru a ve firmwaru, což si studenti ověří na konkrétních laboratorních úlohách. Předmětem je jak symetrická kryptografie (šifry s jedním společným klíčem), tak asymetrická kryptografie (RSA, Kryptografie Eliptických křivek, Diffie-Hellmanova výměna klíčů nad EC). Předmět se dále soustřeďuje na vybrané útoky na kryptografické systémy implementované ve vestavných zařízeních. Studenti tak získají vědomosti o některých potenciálních rizicích kryptografických systémů a budou lépe schopni jim čelit.			
ANIE-COM	Network Communication	Z,ZK	5
Předmět se zaměří na technické aspekty komunikace mezi zařízeními a systémy. V průběhu semestru budou přednášena témata od fyzických vrstev a komunikačních médií až po komunikační protokoly a monitorování provozu. Absolvent předmětu získá přehled o technických omezeních a možnostech komunikačních prostředků, které může využít při návrhu a vývoji reálných hardwarových nebo softwarových systémů.			
ANIE-EHW	Embedded hardware	Z,ZK	5
Předmět poskytuje znalost základních technik a zákonitostí, které řídí konstrukci číslicových zařízení jak malého, tak velkého měřítka. Jsou základem konstrukce pokročilých vestavných systémů, které využívají specializaci své funkce ke konstrukci efektivní hardwarové realizace či podpory výpočtu. Probírají se techniky konstrukce rychlých systémů, jejich standardní vnitřní komunikace, využití přirozeného paralelismu výpočtu ve specializovaných strukturách a systémových architekturách.			
ANIE-ESW	Embedded software	Z,ZK	5
Předmět seznamuje studenty se specifiky vývoje programového vybavení pro vestavné systémy. Předmět studenta provází od základních technik programování v jazyce C a optimalizace kódu, přes řadu typických oblastí, jako je vývoj spolehlivého programového vybavení, vestavné operační systémy či zpracování signálu, až po sofistikované techniky vývoje vestavného programového vybavení kombinované s umělou inteligencí.			
ANIE-MLM	Machine Learning Methods	Z,ZK	5
Předmět seznamuje studenty s metodami strojového učení, které uplatní ve svých specializacích navazujícího programu Aplikovaná informatika. Tyto principy a znalosti nejsou obsaženy ve společném bakářském profilu uchazečů, vyučují se jen ve specializacích zaměřených na umělou inteligenci. Cílem je porozumět teoretickým principům a naučit se prakticky používat modely vhodné pro regresní i klasifikační úlohy ve scénáři učení s učitelem včetně jádrových metod a neuronových sítí. Ve scénáři učení bez učitele se studenti seznámí zejména s modely shlukování a s analýzou hlavních komponent. V předmětu bude také probrána problematika vyhodnocování kvality modelů a základní techniky předzpracování dat. Na cvičeních se k práci s daty a modely budou využívat knihovny pandas, scikit a pytorch pro jazyk Python.			
ANIE-SIM	Digital Circuit Simulation and Verification	Z,ZK	5
Studenti získají podrobné informace o principech kvaziparalelní simulace číslicových obvodů na úrovni RTL (Register Transfer Level) i TLM (Transaction Level Modeling) a o vlastnostech pro tyto účely aktuálně používaných nástrojů. Předmět pokrývá i současné možnosti verifikace, zejména s použitím metodologie UVM (Universal Verification Methodology).			
ANIE-TSP	Testing and Reliability	Z,ZK	5
Studenti získají přehled v oblasti testování číslicových obvodů a o metodách pro zvýšení spolehlivosti a bezpečnosti. Studenti budou schopni vytvořit test obvodu metodou intuitivního zcitlivění cesty, použít automatický generátor testovacích vzorků, budou schopni navrhnout snadno testovatelný obvod a obvod s vestavěným testovacím vybavením. Dále budou schopni analyzovat spolehlivost a provozuschopnost obvodů a aktivně ovlivňovat tyto parametry. Studenti budou schopni navržené znalosti využít v komplexních projektech návrhu obvodů ASIC i FPGA.			
BQM32KOS	Kvantové optické komunikace a sítě	Z,ZK	6
Cílem kurzu je poskytnout komplexní, inženýrský vhled do problematiky optických komunikací se zaměřením na kvantovou distribuci klíče (QKD). Předmět boří hranice mezi tradičními disciplínami a integruje znalosti z vlnové optiky, hardwarové architektury a síťové bezpečnosti. Studenti se naučí chápat komunikační systém jako jeden celek, kde fyzikální vrstva přímo definuje limity a možnosti digitální bezpečnosti. Kurz připravuje na reálné výzvy při nasazování kvantových technologií do stávající telekomunikační infrastruktury.			
BQM36AVM	Adiabatické a variační metody	Z,ZK	6
Kurz představuje adiabatické výpočty a variační kvantové algoritmy (VQA).			
BQM36KPB	Kvantové počítání v bankovnictví	Z,ZK	5
BQM36QTC	Kvantová (stavová, procesní, kanálová) tomografie a kvantové optimální řízení	Z,ZK	6
Kurz představuje klíčové optimalizační problémy v návrhu a analýze kvantových systémů.			
FIT-BIP	Blended Intensive Programme	Z	3
Blended Intensive Program: krátkodobý výjezd přes program Erasmus+			
FIT-PMA	Programování v Mathematica	Z,ZK	4
Systém Wolfram Mathematica patří k nejvýkonnějším nástrojům pro vědecké a technické výpočty, analýzu dat a tvorbu interaktivních modelů. V jednom prostředí spojuje programování, matematiku, vizualizaci, automatizaci i reportování. Je využíván ve výzkumu, průmyslu i technologických společnostech po celém světě od inženýrů v NASA přes analytiky ve fintechu až po datové týmy ve farmaceutickém a automobilovém vývoji. Kurz FIT-PMA studenty provede od základů používání systému Mathematica až k samostatnému řešení složitějších úloh. Naučíte se efektivně kombinovat symbolické a numerické výpočty, psát přehledný a znovupoužitelný kód, pracovat s daty, vytvářet vizualizace a interaktivní dokumenty, automatizovat opakované úlohy a využívat pokročilé výpočetní metody a optimalizace. Důraz je kladen na praktické porozumění principům jazyka Wolfram Language jazyka, který je dnes jedním z nejuniverzálnějších nástrojů pro matematické modelování, datovou analýzu a algoritmický výzkum. Absolventi získají dovednosti využitelné v oblasti vědeckého a technického výzkumu, datové analýzy, softwarového vývoje i výuky matematiky a informatiky. Mathematica je běžně používána v akademických institucích i průmyslu jako prostředí pro rychlou tvorbu prototypů, experimentů a simulací.			
FITE-DIF	Differential equations	Z,ZK	5
This course provides a foundational overview of differential equations, starting with basic motivation and examples of ODEs and progressing to essential solution methods like separation of variables. Key theorems on existence and uniqueness establish when solutions can be guaranteed. Linear and system-based ODEs are covered with methods like characteristic polynomial analysis, followed by examples of non-linear models such as predator-prey and epidemiological models to showcase real-world applications. Finally, an introduction to partial differential equations (PDEs) extends these concepts to multi-variable contexts. The course will also cover numerical methods for solving ODEs and PDEs, including implicit and explicit Euler methods, Runge-Kutta methods, and finite element methods for both ODEs and PDEs.			

FITE-EHD	Introduction to European Economic History	Z,ZK	3
The course introduces a selection of themes from European economic history. It gives the student basic knowledge about forming of the global economy through the description of the key historical periods. As European countries have been dominant actors in this process it focuses predominantly on their roles in economic history. From the large economic area of the Roman Empire to the fragmentation of the Middle Ages, from the destruction of WWII to the current affairs, the development of modern financial institutions is deciphered. The course does not cover the detailed economic history of particular European countries but rather the impact of trade and the role of particular events, institutions and organizations in history. Class meetings will consist of a mixture of lectures and discussions.			
FITE-SEP	World Economy and Business	Z,ZK	4
The course introduces students of technical universities to international business. It does that predominantly by comparing individual countries and key regions of the world economy. Students get to know about different religions and cultures, necessary for doing business in diverse societies as well as indexes of economic freedom, corruption and economic development, which are needed for the right investment decision. Seminars help to improve knowledge in the form of discussions based on individual readings.			
NIE-AIB	Algorithms of Information Security	Z,ZK	5
Studenti se seznámí s algoritmy bezpečného generování klíčů a kryptografickým zpracováním chybových (nejen biometrických) dat. Dále se studenti seznámí s matematickými principy kryptografických protokolů (identifikačních, autentizačních a podpisových schémat). Získají znalosti o metodách detekce malware a použití strojového učení v detekčních algoritmech. Taktéž se seznámí s metodami vytváření steganografických záznamů, s metodami pro jejich vyhledávání a s útoky na ně.			
NIE-AOS	Advanced Operating Systems	Z,ZK	5
Předmět se zabývá problematikou systémového programování v operačních systémech unixového typu se zaměřením na vývoj jádra OS a pokročilými technologiemi pro správu unixových operačních systémů. Studenti se seznámí s architekturou a datovými strukturami jádra OS, se správou procesů a hlavní paměti, s vnitřní architekturou moderních systémů souborů, s implementacemi metod ovládání periferních zařízení a síťové komunikace, s metodami bootování jádra i vlastního operačního systému a s technikami ladění jádra pomocí dynamické instrumentace. Dále získají znalosti o postupech při vývoji a modifikacích jádra OS a zajištění přenositelnosti jádra a o využívání technologií kontejnerizace a virtualizace. Studenti se seznámí se specifikami implementace jádra OS pro vestavné systémy či pro systémy reálného času. Teoretické a obecné principy budou demonstrovány primárně na jádru Linuxu. Cvičení budou zaměřena na vývoj modulů jádra Linuxu a na nástroje pro správu probraných technologií.			
NIE-APR	Selected Methods for Program Analysis	Z,ZK	5
Tento kurz vás seznámí s programovou analýzou, tedy automatizovaným usuzováním o chování počítačového programu. Budeme se zabývat statickou i dynamickou analýzou. Ve statické analýze se podíváme na umění usuzování o programech bez jejich spuštění. Zaměříme se na analýzy pro porozumění programům, optimalizace a detekci chyb. V dynamické analýze se budeme zabývat analýzami, které zohledňují jednotlivé běhy programu v konkrétním prostředí a s konkrétními vstupy.			
NIE-APT	Advanced Program Testing	Z,ZK	5
Testing a program is essential to ensure that a program respects its specification, that changes do not introduce regressions or security issues. The goal of the course is to present advanced program testing techniques, beyond writing unit tests, especially fuzzing and symbolic execution.			
NIE-BLO	Blockchain	Z,ZK	5
Students will understand the foundations of blockchain technology, smart contract programming, and gain an overview of most notable blockchain platforms. They will be able to design, code and deploy a secure decentralized application, and assess whether integration of a blockchain is suitable for a given problem. The course places an increased emphasis on the relationship between blockchains and information security. It is concluded with a defense of a research or applied semester project, which prepares the students for implementing or supervising implementation of blockchain-based solutions in both academia and business.			
NIE-CPX.26	Complexity Theory	Z,ZK	6
Studenti se dozvědí o základních třídách teorie výpočetní složitosti a různých modelech algoritmů a o implikacích této teorie týkajících se praktické algoritmické (ne)řešitelnosti složitých úloh.			
NIE-DSS	Decision Support Systems	Z,ZK	5
The aim of the course is to provide students with knowledge and skills in decision support systems, their classification (Powerova), selected principles of data-oriented, model-oriented and knowledge-oriented decision support systems. Students will also gain knowledge of multicriterial decision-making methods and game theory. They will also learn about the principles of conceptually and ontologically oriented decision support systems and the basics of distribution, optimization and evolution methods and algorithms.			
NIE-DSV	Distributed Systems and Computing	Z,ZK	5
Students are introduced to methods for coordination of processes in distributed environment characterised by nondeterministic time responses of computing processes and communication channels. They learn basic algorithms that assure correctness of computations realized by a group of loosely coupled processes and mechanisms that support high availability of both data and services, and safety in case of failures.			
NIE-EPC	Effective C++ programming	Z,ZK	5
Students learn how to use the modern features of contemporary versions of the C++ programming language for software development. The course focuses on programming effectivity and efficiency in the form of writing maintainable and portable source code and creating correct programs with low memory and processor time requirements.			
NIE-EVY	Efficient Text Pattern Matching	Z,ZK	5
Students get knowledge of efficient algorithms for text pattern matching. They learn to use so called succinct data structures that are efficient in both access time and memory complexity. They will be able to use the knowledge in design of applications that utilize pattern matching.			
NIE-GAK.26	Graph theory and combinatorics	Z,ZK	6
Předmět si klade za cíl seznámit studenta s nejdůležitějšími partiemi teorie grafů, kombinatorických principů a struktur, diskrétních modelů a algoritmů. Kromě pochopení teoretických principů bude kladen důraz i na aplikaci poznatků při řešení úloh a navrhování algoritmů. Mezi probíraná témata patří technika generujících funkcí, vybrané partie z barevnosti grafů a hypergrafů, Ramseyovské věty, úvod do pravděpodobnostních technik a studium vlastností různých speciálních tříd grafů a kombinatorických struktur.			
NIE-GEN	Code Generators	Z,ZK	5
Advanced techniques of translating programs written in high-level programming languages are essential for understanding the field of systems programming. This primarily involves understanding the algorithms and techniques used to translate more complex programming constructs of modern languages employed in systems programming. Students will become familiar with both the theoretical and practical aspects of implementing the back-end of optimizing compilers for programming languages.			
NIE-GPU	GPU Architectures and Programming	Z,ZK	5
Students will gain knowledge of the internal architecture of modern massively parallel GPU processors. They will learn to program them mainly in the CUDA programming environment, which is already a widespread programming technology of GPU processors. As an integral part of the effective computational use of these hierarchical computational structures, students will also learn optimization programming techniques and methods of programming multiprocessor GPU systems.			
NIE-HWB	Hardware Security	Z,ZK	5
The course provides the knowledge needed for the analysis and design of computer systems security solutions. Students get an overview of safeguards against abuse of the system using hardware means. They will be able to safely use and integrate hardware components into systems and test them for resistance to attacks. Students will gain knowledge about the cryptographic accelerators, PUF, random number generators, smart cards, biometric devices, and devices for internal security functions of the computer.			
NIE-KOD	Data Compression	Z,ZK	5
Students are introduced to the basic principles of data compression. They will learn the necessary theoretical background and get an overview of data compression methods being used in practice. The overview covers principles of integer coding and of statistical, dictionary, and context data compression methods. In addition, students learn the fundamentals of lossy data compression methods used in image, audio, and video compression.			

NIE-KRY	Advanced Cryptology	Z,ZK	5
Students will learn the essentials of cryptanalysis and the mathematical principles of constructing symmetric and asymmetric ciphers. They will know the mathematical principles of random number generators. They will have an overview of cryptanalysis methods, elliptic curve cryptography and quantum cryptography, which they can apply to the integration of their own systems or to the creation of their own software solutions.			
NIE-LOM	Linear Optimization and Methods	Z,ZK	5
Students will gain an overview of applications of optimization methods in computer science, economics and industrial practice. They will be introduced to the practical importance of linear and integer programming. They will be able to work with optimization software and to master the languages used in its programming. They will be able to formalise optimisation problems in the areas of computer science (e.g. task allocation to processors, network flow analysis), resource distribution and allocation (traffic problems, business traveller problem, etc.). Gain an overview of computational complexity issues in optimization. Gain a good understanding of linear programming algorithms and selected integer linear programming algorithms.			
NIE-MCC	Multicore CPU Computing	Z,ZK	5
Students will get acquainted in detail with hardware support and programming technologies for the creation of parallel multithreaded computations on multicore processors with shared and virtually shared memory, which are today the most common computing nodes of powerful computer systems. Students will gain knowledge of architecturally specific optimization techniques used to reduce the decrease in computing power due to the widening performance gap between the computational requirements of multi-core CPUs and memory interface throughput. On specific non-trivial multithreaded programs, students will also learn the basics of the art of creating these applications.			
NIE-MKY.26	Mathematics for Cryptology	Z,ZK	7
Studenti získají hlubší znalosti o algebraických postupech řešících nejdůležitější matematické problémy, na kterých je založena bezpečnost šifer. Zejména se jedná o problém řešení soustavy polynomiálních rovnic nad konečným tělesem, problém faktorizace velkých čísel a problém diskrétního logaritmu. Problém faktorizace bude speciálně řešen i na eliptických křivkách. Studenti se rovněž seznámí s moderními šifrovacími systémy založenými na počítání na mřížce.			
NIE-MPS	Modern Computer Networks	Z,ZK	5
Předmět je rozdělen na dvě komplementární části -- moderní síťové technologie a bezpečnost počítačových sítí. První část je věnována popisu principů moderních síťových technologií a komunikačních protokolů, které umožňují dosahovat vysokou propustnost, nízkou latenci a odolnost vůči chybám. Přednášky zahrnují i principy moderních softwarově definovaných sítí, které postupně nahrazují sítě klasické. První část je završena výkladem protokolů a technologií určených pro přenos videa a hlasu v reálném čase. V druhé části jsou nejprve představeny základní principy a technologie podporující a zvyšující bezpečnost počítačových sítí. Následné přednášky jsou věnovány vysvětlení principů známých síťových útoků v lokálních počítačových sítích a v Internetu. Na závěr jsou představeny moderní systémy umožňující detekci a eliminaci síťových útoků, včetně systémů pro sdílení informací umožňujících preventivně síťovým útokům předcházet. Studenti získají praktické zkušenosti s těmito koncepty v síťové laboratoři.			
NIE-PAM	Parameterized Algorithms	Z,ZK	4
There are many optimization problems for which no polynomial time algorithms are known (e.g. NP-complete problems). Despite that it is often necessary to solve these problems exactly in practice. We will demonstrate that many problems can be solved much more effectively than by naively trying all possible solutions. Often one can find a common property (parameter) of the inputs from practice-e.g., all solutions are relatively small. Parameterized algorithms exploit that by limiting the time complexity exponentially in this (small) parameter and polynomially in the input size (which can be huge). Parameterized algorithms also represent a way to formalize the notion of effective polynomial time preprocessing of the input, which is not possible in the classical complexity. Such a polynomial time preprocessing is then a suitable first step, whatever is the subsequent solution method. We will present a plethora of parameterized algorithm design methods and we will also show how to prove that for some problem (and parameter) such an algorithm (presumably) does not exist. We will also not miss out the relations to other approaches to hard problems such as moderately exponential algorithms or approximation schemes.			
NIE-PDL	Practical Deep Learning	KZ	5
This course is designed to provide students with a comprehensive understanding of Deep Learning using PyTorch, a popular open-source machine learning framework. Throughout the course, students will develop practical skills in building and training deep neural networks, using PyTorch to solve real-world problems in fields such as computer vision and natural language processing.			
NIE-PML	Personalized Machine Learning	Z,ZK	5
Personalized machine learning (PML) is a sub-field of machine learning that aims to create models and predictions based on the unique characteristics and behaviors of individual entities. While PML is commonly used in applications such as recommender systems, which recommend items to users based on their personal interests, its principles can be applied to a wide range of other fields, including education, medicine, and chemical engineering. In this course, we will explore the latest PML methods from theoretical, algorithmic, and practical perspectives. Specifically, we will focus on cutting-edge models that are of interest to both the research and commercial communities.			
NIE-REV	Reverse Engineering	Z,ZK	5
Students will learn fundamentals of reverse engineering of computer software (methods of executing and initializing programs, organization of executable files, work with third-party libraries). Special attention will be paid to C ++. Students will also become familiar with the principles of debugging tools, disassemblers and obfuscation methods. Finally, the course will focus on code compression and decompression and executable file reconstruction.			
NIE-RUN	Runtime systémy	Z,ZK	5
As the abstraction level of programming languages steadily rises, modern programs require greater and greater support during their runtime. This course introduces students to various aspects of the runtime support, such as runtime-effective program description, memory management support and garbage collection, just-in-time compilation, and interoperability with other languages and systems.			
NIE-SBF	System Security and Forensics	Z,ZK	5
Students will be introduced to various aspects of system security (principles of endpoint security, principles of security policies, security models, authentication concepts). Students will also learn about forensic analysis as a tool for investigating security incidents (techniques used by malicious software or attackers, forensic analysis techniques, and the importance of memory or file system artifacts for attack analysis and detection).			
NIE-SEM	Semantics of Programming Languages	Z,ZK	5
Cílem předmětu je uvést studenty do základů sémantiky programovacích jazyků, která je základem pro studium a implementaci programovacích jazyků. Tyto techniky jsou také důležité pro verifikaci programů, implementaci optimalizací a obecný návrh programovacích jazyků. Důraz bude na porovnání operační a denotační sémantiky. Použité techniky mají uplatnění i v případě analýzy jazyků daných pouze pomocí operační sémantiky. Kurz umožní studentům získat potřebné dovednosti pro implementaci jazykových konstrukcí, ať už jejich popis pochází z teoretických nebo inženýrských zdrojů v literatuře.			
NIE-SIB	Network Security	Z,ZK	5
The students will gain theoretical and practical knowledge and experience in the area of current security threats in computer networks, specifically about detection and defense. The course explains basic pricipals of security monitoring, packet-based and flow-based analysis, in order to detect anomalies and suspicious network traffic. The course focuses on explanation and practical examples of various mechanisms of securing network infrastructure and detection in real time. The course covers general principals of handling detected security events (i.e. incident handling and incident response).			
NIE-SYP	Parsing and Compilers	Z,ZK	5
The module builds upon the knowledge of fundamentals of automata theory, formal language and formal translation theories. Students gain knowledge of various variants and applications of LR parsing and are introduced to special applications of parsers, such as incremental and parallel parsing.			
NIE-VCC	Virtualization and Cloud Computing	Z,ZK	5
Students will gain knowledge of architectures of large computer systems that are used in data centers and computer infrastructure of companies and organizations. They will get acquainted with virtualization principles, tools and technologies that serve to facilitate and automate configuration, testing and monitoring, and to efficiently operate and optimize the performance parameters of modern computer systems. Theoretically and practically, they will get acquainted with containerization as the most effective technology today for the			

management of complex computer systems and with specific technologies of cloud systems. Finally, they will learn the principles and gain practical skills in the use of modern integration and development tools (Continuous integration and development).

QNIE-AVM	Adiabatic computing and variational methods	Z,ZK	6

The course introduces adiabatic computing and variational quantum algorithms (VQA). We start with a broad introduction to variational methods in physical chemistry (e.g., for calculating ground state of small molecules) and a recapitulation of advances in theoretical computer science (computational complexity and problems such as MAXCUT). We will present the EQA Conjecture and the unique games conjecture. We will present the adiabatic theorem and quantum speedup by quantum annealing (QA). We will build up an understanding of variational quantum algorithms by introducing and analysing, in turn, Variational quantum eigensolver (VQE), Quantum Approximate Optimization Algorithm (QAOA), and their Warm-started variants. As applications, we will highlight variational solvers for systems of linear equations and variational solvers for Markowitz portfolio management, with some discussion of the challenges in benchmarking of VQA.

QNIE-CPX	Teorie složitosti	Z,ZK	6

Students will learn about the fundamental classes of problems in the complexity theory and different models of algoritms and about implications of the theory concerning practical (in)tractability of difficult problems.

QNIE-DIP	Diploma Thesis	Z	30

Independent work of the student under the guidance of the thesis supervisor. Teaching is based on individual consultations with the thesis supervisor or other consultants. The scope of teaching 30 ECTS (i.e. about 900 hours) includes consultations, preparation of theoretical and practical parts of the thesis, writing, preparation for defence and defence of the thesis before the commission. The course supervisor guarantees the quality of the Masters thesis assignment and its compliance with the graduate profile.

QNIE-KKP	Kryptologie a kvantové počítání	Z,ZK	6

The course covers methods and algorithms of cryptology and their relation to quantum computing. In the first introductory lectures, students will be introduced to the basic principles and algorithms of cryptography. Following these topics, students will be introduced to basic cryptanalytic methods. Then some cryptanalytic algorithms running on quantum computers will be presented. In this context, the problem of security of related cryptographic schemes will be discussed. The next lectures will be devoted to post-quantum algorithms. The last lectures deal with cryptosystems using quantum phenomena.

QNIE-KOS	Quantum Optical Communications and Networks	Z,ZK	6

The course focuses on the basic principles and technologies for building and using quantum networks. Students will learn about the key components of quantum networks, including quantum repeaters, routers and switches, and their role in creating a scalable quantum Internet. Emphasis will be placed on quantum cryptography systems. Students will also learn the fundamentals of optics, optical networks, and classical cryptography as they relate to quantum key distribution (QKD) and quantum networks. The course will cover types and architectures of QKD systems (including practical implementation of quantum protocols) according to international standards, key generation and distribution in these systems, and integration of QKD with classical communication systems. Students will also have the opportunity to explore satellite and FSO QKD systems and integrated quantum photonics and electronics.

QNIE-LOM	Lineární optimalizace a metody	Z,ZK	5

Students will gain an overview of applications of optimization methods in computer science, economics and industrial practice. They will be introduced to the practical importance of linear and integer programming. They will be able to work with optimization software and to master the languages used in its programming. They will be able to formalise optimisation problems in the areas of computer science (e.g. task allocation to processors, network flow analysis), resource distribution and allocation (traffic problems, business traveller problem, etc.). Gain an overview of computational complexity issues in optimization. Gain a good understanding of linear programming algorithms and selected integer linear programming algorithms.

QNIE-MPR	Magisterský projekt	Z	7

1. Student si na začátku semestru vybere téma práce (viz Instrukce pro výběr tématu a jeho registraci). S vedoucím si domluví dílčí úkoly, které na zpracování zadání vykoná během semestru. Pokud tyto úkoly splní, udělí mu vedoucí práce na konci semestru zápočet z předmětu NI-MPR. 2. Externí vedoucí práce zadá informaci o udělení zápočtu pomocí formuláře Udělení zápočtu od externího vedoucího závěrečné práce (viz Ke stažení). Vyplněný a podepsaný formulář je potřeba doručit osobně nebo e-mailem referentce pro SZZ, která udělení zápočtu zařídí. 3. Je-li téma práce, které si student rezervoval, formulováno obecněji, měly by úkoly, které mu vedoucí na semestr uloží, směřovat primárně k doladění zadání tak, aby mohlo být zadání práce koncem semestru doplněno a schváleno. Domluva s vedoucím práce, týkající se upřesnění požadavků pro předmět NI-MPR by měla proběhnout v prvních týdnech semestru. Aktivita a odpovědnost leží na studentovi, nikoliv na vedoucím práce. Z hlediska splnění podmínek rozhodně nestačí, aby si student vybral téma. Může dojít k situaci, že se student na konci semestru rozhodne na tématu závěrečné práce dále nepracovat a zvolí si jiné. Stejně tak může vedoucí práce ukončit spolupráci se studentem. I v tomto případě je možné udělit zápočet.

QNIE-MQI	Matematika pro kvantovou informatiku	Z,ZK	6

Linear algebra on finite dimensional spaces with scalar product, Hilbert spaces, Dirac's bra-ket formalism, normal, Hermitian and unitary operators, operator spectrum, orthonormalization, diagonalization, matrix exponential, tensor product of vector spaces and operators. Discrete Fourier transform and fast Fourier transform.

QNIE-NMK	Numerical methods for quantum computation	Z,ZK	5

The course is devoted to numerical solution of boundary-value problems and intial-boundary-value problems for ordinary and partial differential equations. It explains finite-difference, finite-element and finite-volume methods for elliptic, parabolic and hyperbolic partial differential equations. Students are introduced to the recent advances in methods solving the mentioned problems.

QNIE-OPM	Optical measurements	Z,ZK	6

The aim of this course is to acquaint students with optical measurement methods from the detection of microparticles, non-regulation and surface breaches, through the use of fiber optics in areas where it is not possible to use standard electronic sensors, or in places with increased risk of explosion and in hospitals, lidars used in intelligent transport infrastructures, to macroscopic sensing (remote sensing) of the Earth, atmosphere and space. The inclusion of these measurement methods requires in particular an understanding of the physical mechanisms on which they are based, as well as knowledge of measurement procedures and specifics in data processing and reconstruction.

QNIE-OQC	Optical quantum computing	Z,ZK	5

The course covers the basic theoretical methods and concepts for optical quantum computing, complemented by on hands-on exercise and applications using quantum programming libraries, Strawberry Fields and Piquasso. Theoretical concepts include measurement-based quantum computation, Gaussian Boson Sampling, and quantum supremacy. Applications feasible on current and near-term hardware include recent generative and discriminative machine-learning algorithms, as well as molecular vibration simulations.

QNIE-OVV	Optimization for Scientific Computing	Z,ZK	5

The content of the course is an explanation of numerical methods for solving nonlinear optimization, convex optimization, stochastic optimization, optimal control, applications for QC, genetic and evolutionary programming, machine learning, deep neural networks. Students are also introduced to modern trends in solving these problems.

QNIE-PJK	Programming languages for quantum computing	Z,ZK	5

Computational models for quantum computing: quantum Turing machine, QRAM, lambda calculus with qubits. Higher programming languages for quantum computation: imperative languages (Silq), functional languages (QML, Quipper).). In the seminars the student will learn the basics of programming in the higher programming language Silq.

QNIE-PNM	Parallelization of numerical methods	Z,ZK	5

The content of the course is an explanation of numerical methods for solving mathematical models with a focus on their parallelization and the use of these methods in QC. Students are also introduced to modern trends in the field of solving these problems.

QNIE-PON	Selected Topics in Optimization and Numerical mathematics	Z,ZK	5

Students will be introduced to special optimization problems that arise in the field of machine learning and artificial intelligence and will extend the basic knowledge of continuous optimization acquired in previous studies. They will also learn about the details of implementing solutions to these problems on a computer and related mathematical concepts, especially from numerical linear algebra.

QNIE-PPS	Programování paralelních systémů	Z,ZK	6
Nowadays, multi-core processors and GPU accelerators have become common components of computing clusters and high-performance computing systems, so knowledge and skills related to parallel programming are essential for every computer scientist. The aim of this course is to introduce students to the architectures and programming methods of parallel computers with shared memory, GPU accelerators, or with distributed memory. To effectively use these modern computing systems, it is essential to combine parallelization techniques at all three levels. Students will gain knowledge of the relevant programming models, languages and environments. They will become familiar with fundamental parallel algorithms and be able to analyze the limitations, efficiency, and scalability of parallel solutions to selected problems on high-performance computing systems. In addition to the necessary theory in lectures, students will gain practical experience and skills in programming in OpenMP, CUDA and MPI environments.			
QNIE-QC1	Kvantové výpočty 1	Z,ZK	6
The course introduces the student to basic principles of quantum computation and shows the difference between classical and quantum mechanics. Quantum computation uses quantum circuits, which will be demonstrated in the Qiskit SDK. The course will gradually introduce the student to such concepts the state of a quantum system and its visualization, measurements, basic gates and their composition, and the so-called entanglement. The student will be introduced to the BB84 and E91 protocols as demonstrations of the properties of quantum states. The course will also cover quantum teleportation, quantum oracle queries, the Deutsch-Jozsa algorithm, the quantum Fourier transform, the phase estimation algorithm, and the Shor algorithm.			
QNIE-QC2	Kvantové výpočty 2	Z,ZK	6
Quantum Computing 2 focuses on advanced quantum algorithms and their implementations: the Grover algorithm and its applications, quantum algorithms solving linear algebra problems, HHL for solving systems of linear equations. In the course we also introduce students to variational methods and error correction.			
QNIE-QEC	Quantum error correction	Z,ZK	5
In this course, we will build a theory for the construction of quantum error-correcting codes. In the introductory part, necessary chapters from the classical theory will be summarized, atop of which we then present the quantum analogy. We will show how coherently stored quantum information can be made robust to loss and noise. We conclude the course by arriving at the principle of fault tolerance, based on which quantum computers are able to continuously correct errors arising at runtime and thus achieve correct results even with erroneous bits, gates or measurements.			
QNIE-QML	Quantum machine learning	Z,ZK	5
The aim of the course is to introduce students to quantum machine learning. Students will first learn theoretically and practically about the quantum representation of classical data. Next, they will explore kernel methods, the quantum SVM model, and the use of quantum variational methods in supervised learning scenarios. The course will also introduce quantum neural networks and quantum generative adversarial models in unsupervised learning scenarios. The primary focus of the course is quantum algorithms for classical data. The exercises will use the pandas and qiskit libraries for Python to work with data and models.			
QNIE-QOM	Quantum Optics, Metrology, Sensing and Imaging	Z,ZK	5
Students are given an introduction to the quantum theory of light and related fundamental principles with an emphasis on practical aspects. They acquire the theoretical and experimental foundations for the development of specifically quantum mechanical approaches to metrology and imaging in quantum computing and communications. Specific problems discussed include elementary processes with photons (absorption, emission, stimulated emission), interference, entanglement, non-classical phenomena with photons, methods of suppressing optical aberrations and dispersion. The various techniques are explained theoretically and also using experiments that demonstrate these principles in practice.			
QNIE-TIN	Teorie informace	Z,ZK	6
The course focuses on the mathematical description of a random message source, its coding and transmission of the source through a noisy channel. The coding problem is addressed probabilistically, the relation of the mean length of the optimal code with the entropy and entropy rate of the random source is emphasized. In the case of the noisy channel we focus on the set of typical sequences and its appropriate coding by self-correcting codes. The course includes a reminder of necessary concepts such as conditional distributions, goodness-of-fit and independence tests, and an introduction to random chains.			
QNIE-UKT	Úvod do kvantové teorie	Z,ZK	6
interpretation of quantum theory are explained using simple models mainly from finite-dimensional quantum mechanics. Emphasis is placed on further applications of quantum theory to information processing and communication. Possible physical realizations of a qubit, description of multipartite systems, quantum entanglement and its applications are discussed. The course concludes with a description of continuous quantum systems in infinite-dimensional Hilbert spaces, in particular the linear harmonic oscillator as a description of the mode of a quantized electromagnetic field.			

Aktualizace výše uvedených informací naleznete na adrese http://bilakniha.cvut.cz/cs/FF.html
Generováno: dne 09.09.2026 v 20:15 hod.