ENTRANCE EXAMINATION PROGRAM
FOR PHYSTECH SCHOOL OF RADIO ENGINEERING AND COMPUTER TECHNOLOGY
COMPUTER SCIENCE AND INFORMATICS
COMPETITIVE GROUP
FOR APPLICANTS ENTERING PHD PROGRAMS

The exam ticket includes 2 questions. The first question is from the section of the program corresponding to the scientific specialty in which the applicant intends to study. The second question is about the applicant's future dissertation work: subject, existing groundwork, presence of a supervisor, publications. Questions can also be asked about the content of the final qualifying work (master's or specialist's).

1 hour is given for preparation and it is allowed to use books, with the exception of electronic media. It is not allowed to use different means of communication or the Internet. The applicant answers the exam ticket in the form of an oral interview, during which additional questions on the relevant section of the program may be asked.

Section 1. Mathematical modeling, numerical methods and software packages

1. Solution of systems of nonlinear equations. Newton's method. Theorem on the quadratic rate of convergence. Simple iteration methods, convergence analysis. Continuation method by parameter.
2. Numerical differentiation. Basic difference approximations of the first and second derivatives. Approximation error, rounding error. The optimal step of numerical differentiation. Grid method for the heat equation. The simplest difference schemes (explicit, implicit). Approximation of equations, initial and boundary conditions. Explicit schema implementation. Layer count. Implementation of the implicit scheme, the equation on the upper layer, its solution by the sweep method.
3. Numerical integration of the Cauchy problem for ODE systems. Grid method, simplest difference schemes (Explicit and implicit Euler schemes, central difference scheme). Implementation of difference schemes. Approximation error, criteria for small grid spacing.
4. Typical problems of computational linear algebra. Matrix analysis. Perturbation theory and condition numbers. Calculations with finite precision.
5. Triangular systems. LU decomposition. Symmetric matrices. Band matrix. Sparse matrix. LDMT and LDLT expansions. Orthogonal matrices. Householder and Givens matrices. QR decomposition. SVD decomposition.
6. The problem of eigenvalues. Hessenberg form and Schur form. Perturbation theory. Robust QR method. Symmetric QR method and SVD.
7. Convex optimization and duality. Extremum conditions in smooth problems, Levitin-Milyutin-Osmolovsky theorem. Duality in convex and linear programming.
8. Pontryagin's maximum principle in the calculus of variations and optimal control.
9. Lagrange's principle for smooth-convex problems. Lagrange principle in the theory of optimal control.
10. Basic concepts and tasks of statistical estimation. Exponential and observable families of distributions. Plausibility. Statistical theory of decision making.
11. Bayesian inference. Comparison of Bayesian and frequentist approaches to statistical estimation. Bayesian decision theory. Exclusion of interfering parameters. permutability. De Finetti's theorem.

12. Asymptotic normality of the posterior distribution. Doob's theorem. Ibragimov – Khasminskii conditions. Consistency of Bayesian estimates. Bernstein-von Mises theorem.
13. Linear regression analysis. Ordinary and generalized least squares methods. Estimation of linear model errors. Testing hypotheses about the parameters of the linear model. Confidence intervals.
14. Nonlinear regression analysis. Basic methods of non-parametric regression (multivariate non-parametric regression, neural networks, radial basis functions, regression based on the support vector system, kriging).
15. Statement of the problem of dimension reduction. Linear methods of dimension reduction. Principal component analysis. Multidimensional scaling.
16. Statement of the problem of classification. Bayesian classifier. Linear classifiers: perceptron. Rosenblatt's algorithm. Support vector machine. Optimal hyperplane. Algorithm for constructing the optimal hyperplane. Estimation of the generalization error probability in terms of the number of support vectors.
17. Vapnik–Chervonenkis generalization theory. VC-dimension, definition, main property. Upper bound on the classification error probability in terms of the VC-dimension of a class of classification functions.
18. The problem of universal online forecasting: a statistical approach. Calibration of forecasts. Algorithm for computing well calibrated predictions.
19. Elements of the theory of algorithms. Turing machines, Post machines, normal Markov algorithms. Estimates of the complexity of algorithms. NP - Tasks (algorithms).
20. Elements of the theory of languages. Finite automation - automaton grammars, pushdown automata - context-free grammars.
21. Algorithms on graphs. The concept of a graph. Special classes of graphs. Search on graphs in breadth, in depth. Algorithms for finding the minimum path.
22. Object = data + methods for working with them. Abstraction as a means of modeling reality with the help of objects. Encapsulation. Modification and optimization of programs using encapsulation. Inheritance. Code reuse. Polymorphism as a means of ensuring the extensibility of programs. The concept of an interface as an alternative means of providing polymorphism.
23. Dynamic arrays, lists and their comparison. Queue and stack. The concept of mapping. Implementation of mappings through binary trees and hash tables. Concepts of dynamic objects and heaps. Basic heap operations. Garbage collection.
24. DBMS. Logical and physical data structure. Means of ensuring data integrity. Transactions. Relational data model. Data normalization. ER - diagrams. SQL language. Data warehouses. Comparison with operational databases. Denormalization. Multidimensional data model. OLAP. Data marts. Their use as an intermediate layer in a three-tier architecture.
25. The concept of architecture of distributed computing systems. Computer networks. Seven-layer model of open systems interaction (OSI Seven - Layer Model). The concept of client-server. Examples of its application.

Section 2. Theoretical informatics, cybernetics

1. General principles of modeling the processes of human thinking and human-machine communication. Machine representation of knowledge and data. Methods for storing, searching and processing data, methods of natural language human-machine communication
2. Transfer of information. Model of the communication system and the role of each of the blocks. Shannon’s measures of information: intrinsic information, entropy, mutual information.
3. Statistical sources with and without memory. Entropy of a stationary source. Limiting average and conditional entropies.
4. Coding the source of information. Shannon's theorems for the source. Separable and inseparable codes. Prefix code. McMillan's theorem. Kraft's inequality.

5. Shannon, Fano, Huffman codes. Universal coding: Lempel-Ziv-Welch algorithms, Lempel-Ziv algorithm. Arithmetic coding.
6. Coding for channel: Classification of channels. The Information processing lemma and the Fano's bound. Channel capacity. Symmetrical channel without memory, its parameters and characteristics. Calculation of the bandwidth of channels, taking into account the symmetry of the inputs and outputs.
7. Decoding as a division of the entire signal area at the channel output into separate sub-areas. Decoding with and without decision failure. Decoding errors.
8. Shannon's direct and inverse theorems. Error probability exponent for a memoryless binary symmetric channel.
9. Continuous sources and continuous channels. Nyquist-Shannon sampling theorem.
10. Finite fields, vector spaces. Groups, rings and fields. Rings of polynomials. Euclid's algorithm.
11. Block codes. Singleton, Plotkin, Elias Bassalygo, Hamming, Gilbert-Varshamov boundaries.
12. Cyclic codes. Systematic form of generating and checking matrices.
13. Bose-Chowdhury-Hokvingham codes. Reed-Solomon codes. Algebraic decoding of Reed-Solomon codes.
14. Convolutional codes. Viterbi algorithm. Turbo codes and low-density parity codes.
15. Rank codes. Matrix and vector representation. Singleton border. Decoding algorithms.
16. Information as a subject of protection. Features of information as a subject of protection. Scenarios for the exchange of information between two parties: ensuring confidentiality; integrity assurance (hash functions).
17. Ensuring message authentication and identification of parties (protocols); ensuring the impossibility of refusal of authorship by the transmitting party and the impossibility of forgery by the receiving party (digital signature, hash functions).
18. Modulo comparisons. Fermat's little theorem. Euler function. Chinese remainder theorem.
19. The complexity of the algorithms for addition, multiplication, raising to an integer power.
20. Cryptography and cryptanalysis. Encryption keys. Assumptions in cryptanalysis. Cryptographic strength of the information security system.

Section 3. Artificial intelligence and machine learning

1. Definition of artificial intelligence. Strong and weak AI.
2. Logical, functional, agent-based approach to AI. Intelligent agents.
3. Knowledge bases. Expert systems. Knowledge engineering.
4. Self-learning systems. Logical approach to learning.
5. Decision making in the face of opposition. Game intelligence.
6. Computer vision.
7. Tasks of sound recognition and understanding of oral speech.
8. Swarm and ant intelligence.
9. Biological neuron. Neurotransmitters. Polarization and depolarization. Action potentials (spikes).
10. The simplest formal McCulloch-Pitts neuron.
11. Definition of a neural network (NN). Types of NN architecture.
12. Rosenblatt's receptor.
13. Rumelhart perceptron. Perceptron learning theorem. Linear separability constraint.
14. Feed-forward networks. Kolmogorov's completeness theorem.
15. Backpropagation algorithm.
16. First order algorithms: delta-bar-delta, extended delta-bar-delta (EDBD).
17. Newton's method for learning NN.
18. Quasi-Newtonian methods of the second order: Levenberg-Marquardt, Polak-Ribière, BFGS, etc.

19. Methods for finding the global minimum of the error functional. Random starts. annealing method.
20. Genetic algorithms in NN learning.
21. Kohonen self-organizing map.
22. Neural associative memory. Hopfield networks.
23. Bidirectional associative memory. Pseudo-inverse associative memory.
24. Nuclear methods in machine learning. Support vector machine. Nuclear associative memory.
25. Recurrent neural networks. Backpropagation through time (BPTT) algorithm.

Section 4. Cybersecurity

1. Principles of multilevel and layered protection of information in computer networks.
2. Complex application of cryptographic algorithms and systems in computer networks.
3. Crypto providers. Principles of construction and use of the cryptographic interface CryptoAPI.
4. Tasks and procedures for managing public keys.
5. Legal regulation of public key management. The need to protect public keys. General provisions on certification and certificates.
6. General provisions on the use of public key digital certificates. General information about the structure of a public key digital certificate.
7. Signs and main stages of the implementation of computer attacks.
8. Systems for detecting and preventing computer attacks and their classification. Requirements for systems for detecting and preventing computer attacks.
9. Security analysis systems: classification, architecture. Requirements for security analysis systems.
10. Methodology for analyzing the security of an automated system.
11. Purpose and functions of firewalls. Classification of firewalls and their characteristics.
12. Generalized block diagram of the firewall. Basic schemes for connecting firewalls.
13. Organization of secure internetworking and remote access.
14. Protection of information exchange at the data link level.
15. Purpose and structure of the IPSec protocol family.
16. Format of IKE, AH and ESP protocols.
17. System of protection of information services of a computer network.
18. Approaches applied to ensuring information security in client-server information and computing systems.
19. Types of authentication and differentiation of access to information services.
20. Architecture of SSL and TLS data protection protocols. The procedure for negotiating session parameters.
21. Features of cryptographic calculations in the SSL and TLS protocols.
22. Cryptographic authentication and authorization protocol Kerberos.
23. Purpose, composition and capabilities of the e-mail protection system.
24. Functionality of S/MIME email security software.
25. Threats to the security of information in databases. Information security system in DBMS. Access control mechanisms in DBMS.

References

Mathematical modeling, numerical methods and software packages

1. Федоренко Р.П. Введение в вычислительную физику. – М.: Наука, 1994.

2. Каханер Д., Моулер К., Нэш С.. Численные методы и программное обеспечение. — М.: Мир, 1998.
3. Бахвалов Н.С., Жидков Н.П., Кобельков Г.М. Численные методы. 5-е изд. – М.: БИНОМ. Лаборатория знаний, 2007 – 636 с.
4. Голуб Дж., Ван Лоун Ч. Матричные вычисления. Мир, 1999. – 548 с.
5. Деммель Дж. Вычислительная линейная алгебра. Теория и приложения. Мир, 2001. – 435 с.
6. Магарил-Ильяев Г.Г., Тихомиров В.М. Выпуклый анализ и его приложения. Изд-е 3-е. М.: УРСС, 2011.
7. Ибрагимов И.А., Хасьминский Р.З. Асимптотическая теория оценивания. М.: Наука, 1979.
8. V. Spokoiny. Basics of Modern Parametric Statistics. Springer, 2013 (см. http://premolab.ru/sites/default/files/stat.pdf).
9. Арутюнов А.В., Магарил-Ильяев Г.Г., Тихомиров В.М. Принцип максимума Понтрягина. Доказательство и приложения. М.: Факториал Пресс, 2006.
10. Айвазян С.А., Бухштабер В.М., Енюков С.А., Мешалкин Л.Д. Прикладная статистика. Классификация и снижение размерности. М.: Финансы и статистика, 1989.
11. Вьюгин В.В. Элементы математической теории машинного обучения. М.: Московский физико-технический институт (государственный университет) – ИППИ РАН, 2010. – 232
12. Кормен Т. Х., Лейзерсон Ч. И., Ривест Р. Л., Штайн К. Алгоритмы: построение и анализ.– 2-е изд. – М.: Издательский дом «Вильямс», 2006.
13. Ахо А., Хопкрофт Дж., Ульман Дж. Структуры данных и алгоритмы. – М.: Издательский дом «Вильямс», 2000.
14. Вирт Н. Алгоритмы и структуры данных. – СПб.: Невский Диалект, 2005.
15. Керниган Б., Ритчи Д. «Язык программирования Си», 2-е издание, пер. с англ., М.: Финансы и статистика, 1992.
16. Страуструп Б. Язык программирования С++, 3-е издание, пер. с англ. - СПб.: Невский диалект, 1999 г.
17. Карпов В.Е., Коньков К.А. Основы операционных систем. Курс лекций. Учебное пособие. – М.: ИНТУИТ.РУ «Интернет-Университет Информационных Технологий, 2005.
18. Гарсиа-Молина Г., Ульман Дж., Уидом Д. Системы баз данных. Полный курс. М.: Вильямс, 2004.
19. Якобсон А., Буч Г., Рамбо Дж. Унифицированный процесс разработки программного обеспечения. СПб.: Питер, 2002.

Theoretical informatics, cybernetics

1. Габидулин Э. М., Пилипчук Н. И. Лекции по теории информации: Учебное пособие. – М.: МФТИ, 2007.
2. Попов, И. Ю. Теория информации : учебник / И. Ю. Попов, И. В. Блинова. — Санкт-Петербург : Лань, 2020. — 160 с. — ISBN 978-5-8114-4204-1.
3. Сагалович Ю.Л. Введение в алгебраические коды: Учебное пособие. – М.: МФТИ. 2007.
4. Габидулин Э.М., Кшевецкий А.С., Колыбельников А.И. Защита информации: Учебное пособие. – М.: МФТИ, 2017. – 262 с.

Artificial intelligence and machine learning

1. С. Расселл, П.Норвиг. Искусственный интеллект. Современный подход. Вильямс. 2006г.
2. Bishop, Christopher M. Pattern recognition and machine learning. Vol. 4. No. 4. New York: springer, 2006.
3. С. Осовский. Нейронные сети для обработки информации. М., «Финансы и Статистика», 2004
4. Хайкин, Саймон. Нейронные сети: полный курс, 2-е издание. Издательский дом Вильямс, 2008.
5. Дж.Ф. Люгер. Искусственный интеллект. Стратегии и методы решения сложных проблем. Вильямс. 2003 г.
6. Саттон Р.С., Барто Э.Г. Обучение с подкреплением. — БИНОМ, 2011

Cybersecurity

1. Стародубцев, Ю. И. Комплексная защита информации в локальных вычислительных сетях / Ю. И. Стародубцев, В. Е. Дементьев, М. А. Коцыняк. – Санкт-Петербург: ВАС, 2010. – 436 с.
2. Шангин, В. Ф. Комплексная защита информации в корпоративных системах: учебное пособие / В. Ф. Шангин. – Москва: ИД "Форум", 2010. – 592 с.
3. Запечников, С. В. Информационная безопасность открытых систем: учебник для вузов. В 2-х т. Т. 2. – Средства защиты в сетях / С. В. Запечников, Н. Г. Милославская и др. – Москва: Горячая линия – Телеком, 2008. – 558 с.
4. Свечников, Д. А. Межсетевые экраны. В 2 ч. Ч. 1. / Д. А. Свечников и др. – Орёл: Академия ФСО России, 2013. – 170 с.
5. Комашинский, В. В. Методика применения криптопровайдеров для защиты прикладного программного обеспечения: учебно-методическое пособие / В. В. Комашинский. – Орёл: Академия ФСО России, 2010. – 182 с.
6. Свечников, Д. А., Комашинский, В. В. Яшин, А. А. Методические рекомендации по разработке программ для криптографической защиты информации / Д. А. Свечников, В. В. Комашинский, А. А. Яшин. – Орёл: Академия ФСО России, 2011. – 110 с.
7. Комашинский, В. В. Инфраструктура управления открытыми ключами: пособие / В. В. Комашинский. – Орёл: Академия ФСО Рссии, 2010. – 230 с.: ил.
8. Основы информационной безопасности: учебое пособие / А. И. Козачок, А. А. Юркин, Н. И. Биркун и др.; под ред. В. И. Козачка. – Орёл: Академия ФСО России, 2009. – 302 с.
9. Беляев, Д. Л. Компьютерная безопасность: практикум. В 2 ч. Ч. 1 / Д. Л. Беляев, В. В. Комашинский. – Орёл: Академия ФСО России, 2008. – 144 с.
10. Галицкий, А. В. Защита информации в сети – анализ технологий и синтез решений / А. В. Галицкий, С. Д. Рябко, В. Ф. Шаньгин. – Москва: ДМК Пресс, 2004. – 616 с.: ил.

11. Платонов, В. В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей: учебное пособие для вузов / В. В. Платонов. – Москва: Академия, 2006. – 240 с.: ил.
12. Хорев, П. Б. Методы и средства защиты информации в компьютерных системах / П. Б. Хорев. – Москва: Академия, 2008. – 256 с.
13. Защита от несанкционированного доступа к информации и требования по защите информации. Автоматизированные системы. Классификация автоматизированных систем и требования по защите информации. Гостехкомиссия России. Руководящий документ. – Москва: Военное издательство, 1992. – 27 с.
14. Защита от несанкционированного доступа к информации. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Ч. 1. Гостехкомиссия России. – Москва: Военное издательство, 1999. – 6 с.
15. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Гостехкомиссия России. Руководящий документ. – Москва: Военное издательство, 1992. – 9 с.
16. Шугуров, Д. Е. Методы и протоколы аутентификации / Д. Е. Шугуров и др. – Орёл: Академия ФСО России, 2013. – 219 с.
17. Международный стандарт ISO/IEC IS 27001:2005. Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования. – Москва: ООО "GlobalTrust Solutions", 2005.
18. ГОСТ Р ИСО / МЭК 15408–2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 1. Введение и общая модель. Ч. 2. Функциональные требования безопасности. Ч. 3. Требования доверия к безопасности.
19. Комашинский, В. В. Управление доступом в компьютерных системах / В. В. Комашинский и др. – Орёл: Академия ФСО России, 2013. – 115 с.
20. Афанасьев, А. А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам: учебное пособие для вузов / А. А. Афанасьев, Л. Т. Веденьев, А. А. Воронцов и др.; под ред. А. А. Ше-лупанова, С. Г. Груздева, Ю. С. Нахаева. – Москва: Горячая линия – Телеком, 2009. – 552 с.: ил.
21. Чипига, А. Ф. Информационная безопасность автоматизированных систем: учебное пособие для студентов вузов, обучающихся в обл. информ. безопасности / А. Ф. Чипига. – Москва: Гелиос АРВ, 2010. – 336 с.: ил.
22. Черемушкин, А. В. Криптографические протоколы. Основные свойства и уязвимости: учебное пособие для студ. учреждений высш. проф. образования / А. В. Черемушкин. – Москва: Издательский центр "Академия", 2009. – 272 с.
23. Гостехкомиссия России. Руководящий документ "Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации". – Москва: Военное издательство, 1997.
24. Поляков, А. М. Безопасность Oracle глазами аудитора: нападение и защита. – Москва: ДМК Пресс, 2010. – 336 с.: ил.