AL-FARABI KAZAKH NATIONAL UNIVERSITY

FACULTY OF INFORMATION TECHNOLOGIES

Approved at the meeting of the Scientific
and methodological Council of
al-Farabi Kazakh national University
protocol №_____
from «_____» _____ 2020 y

ENTRANCE EXAM PROGRAM
FOR APPLICANTS TO THE PhD PROGRAM IN THE SPECIALTY
"8D06301- Information Security Systems "
(for 3 years.)

ALMATY 2020

The program is compiled in accordance with the State educational standard for the specialty "8D06301- Information Security Systems ". The program was compiled with acting Professor Mussiraliyeva Sh. Zh.

The program was reviewed at the meeting of the Department of Information systems
Protocol № ____ "____ " _____ 2020y.

Head of Department _____ Mussiraliyeva Sh. Zh.

Approved at the meeting of the method Bureau of the faculty of information technology
Protocol № ____ "____ " _____ 2020y.

Chair method of the Bureau _____ Gusmanova F. R.

Approved at the meeting of the Academic Council
Protocol № ____ "____ " _____ 2020y.
Chairman of the Academic Council,
Dean of the faculty _____ Urmashev B. A.

Academic Secretary _____ Sambetbaeva A. K.

PROGRAM CONTENT

1. Goals and objectives of the entrance exam in the specialty

1.1. The purpose of the entrance exam in the specialty

The purpose of the entrance exam is to identify the level of theoretical training entering the doctoral program and the formation of a personal recommendation for admission on the basis of competitive participation.

The program of the entrance exam includes the following disciplines: “Organization of information security systems”, “Methods and means of protecting computer information”, “Elements of information protection means”

1.2 Tasks of the entrance exam in the specialty

During the exam revealed:

• The applicant's knowledge of the fundamental principles of computer science and information technology; main achievements and development trends of modern computer science; technologies of professional and scientific activity; knowledge of the main provisions of professional and scientific ethics and their use in work.

• Ability to find, analyze and process scientific, technical, natural-scientific and general scientific information, leading it to a problem-task form; design and carry out their professional, scientific and scientific-pedagogical activities; to design your further professional development.

• Skills of independent research work and research work; scientific project activities, the solution of standard scientific and professional tasks, the correct and logical design of their thoughts in oral and written form.

2. Requirements for the level of training of people entering PhD doctor studies

Previous level of education:
academic master's degree in the field of:
6M070300 – Information Systems
6M100200 – Information Security Systems
6M060200 – Informatics
6M011100 – Computer Science
6M070200 – Automation and control
6M070400 – Computer Engineering and Software
6M060300 – Mechanics
6M070500 – Mathematical and computer modelling
6M060100 – Mathematica
6M071900 – Radio engineering, electronics and telecommunications

Applicants must have a state document of the appropriate level of education.

The program of entrance exam for applicants for doctoral studies in the direction of preparation “8D06301 – Information Security Systems” was developed at the Department of “Information Systems”.

3. Prerequisites for the educational program

Prerequisites:

1. Organization of information security systems;
2. Methods and means of protecting computer information;
3. Elements of information security tools.

4. Exam Topics

Discipline "Organization of information security systems"

1. Classic ciphers and their opening. The shift cipher and the affine cipher and their decryption and hacking by brute force. Frequency method of opening the replacement cipher. The disadvantages of classical ciphers, the frequency analysis of such ciphers of texts in Kazakh and

Russian languages.

2. Ring of integers, Euclidean algorithm and consequences. Representation of the greatest common divisor. Theory of Comparisons. Comparison properties for this module. Reversible elements for this module.

3. Euler function and its properties. Euler function on primes. The theorem on the multiplicativity of the Euler function. The formula for finding the values of the Euler function, exponentiation using the Euler function.

4. Fermat-Euler theorem and the main theorem of the RSA cipher.

5. RSA cipher, encryption and reading process, rationale. RSA encryption with the public key of the specified text. RSA decryption of the specified text with the private key.

6. RSA-electronic signature, idea and rationale.

7. Implementation of the RSA-electronic signature procedure, part of the signing of the document by electronic signature.

8. Implementation of the RSA-electronic signature procedure, part of the public key signature encryption.

9. The distribution of primes in a natural series and the evaluation of the RSA cipher.

10. The ring of polynomials over the field $< F_2^n$ **; +,* >** Euclidean algorithm, representing the greatest common divisor of two polynomials. Irreducible polynomials in this ring. Irreducible polynomials of degrees 2,3,4,5.

11. Field construction $< F_2^n$ **; +,* >** as fields constructed from residues modulo an irreducible polynomial. The addition and multiplication task in this field. Inverse elements of addition and inverse elements of multiplication for nonzero elements of this field. Build field **<** F_{16} **; +, * >**.

12. The Lagrange theorem on the divisibility of the order of a group by the order of a subgroup. The corollary is that the order of an element divides the order of the group. Examples of subgroups of Zn. The antiderivative element theorem in the field $< F_{2n}$; +,* >. Primitives of the field $< F_{16}$; +,* >.

13. The construction of a field constructed from n-bit binary blocks. The addition and multiplication task in this field. Inverse elements of addition and inverse elements of multiplication for nonzero elements of this field, primitive elements of this field. Build a field of 4-bit binary blocks, specify the primitive elements of this field.

14. The Difi-Hellman problem. Creating a shared secret for remote users, relying on the "unsolvability" of the Dhifi-Hellman problem. Solving the key exchange problem for remote users.

15. Al-Gamal cipher, key exchange precess, encryption and decryption. Implementation by example.

References:

Basic:

1. Яблонский С.В. Введение в дискретную математику. М.: Высшая школа, 2010. – 381 с.

2. Черёмушкин А.В. Лекции по арифметическим алгоритмам в криптографии. М.: МЦНМО, 2012.

3. Кормен Т., Лейзер Ч., Риверс Р. АЛГОРИТМЫ: построение и анализ. М.: МЦНМО, 2010. – 900 с.

4. А. П. Алферов т.б. Основы криптографии. Москва, «Гелиос АРВ», 2002 ж.

5. В. И. Нечаев, ЭЛЕМЕНТЫ КРИПТОГРАФИИ. Основы защиты информации. М., Высшая школа, 1999 г.

Additional:

1. А. А. Бухштаб. Основы теории чисел. М.: Просвещение, 1966.

2. D. R. Stinson. KRIPTOGRAPHY, Teory and Practice. CRC Press, Boca Raton, 1995.

Discipline "Methods and means of protecting computer information"

1. Brief historical information about the emergence and development of cryptology methods. Cryptography. Confidentiality. Integrity. Authentication Digital signature.
2. The Bell-Lapadula Model. Pre-distribution of keys. Key forwarding. Open key distribution. Secret sharing scheme. Public Key Infrastructure Certificates Certificate Authorities. Formal cipher models. Plaintext models. Mathematical models of plaintext. Clear text recognition criteria. Classification of ciphers according to various criteria. The mathematical model of the replacement cipher. Classification of replacement ciphers.
3. Model Low-Water-Mark (LWM). Route permutations. Elements of crypto-analysis of permutation ciphers. Replacement Ciphers.
4. Models J. Goguen, J. Meseguer. Table gamming. On the possibility of restoring the probabilities of gamma signs. Recovering texts encrypted with an unequal probability. Reuse of gamma. Cryptanalysis of the Vigenere cipher. Encryption errors.
5. Security breach detection model. Entropy and redundancy of the tongue. The distance of uniqueness. Strength of ciphers. Theoretical resistance of ciphers. Practical durability of ciphers. Issues of resistance to ciphers. Distortion-free ciphers. Ciphers that do not propagate distortions such as "replacement of characters. Ciphers that do not propagate distortions such as" skip-insert characters.
6. Block encryption systems. The principles of building block ciphers. Examples of block ciphers. American data encryption standard DES. Data encryption standard GOST 28147-89. Modes of using block ciphers. Combination of block cipher algorithms. Methods of analysis of block encryption algorithms. Recommendations for using block cipher algorithms.
7. Stream encryption systems. Synchronization of stream cipher systems. The principles of building stream cipher systems. Examples of stream cipher systems. Encryption system A5. Gifford cipher system. Linear shift registers. Berlekamp – Messi Algorithm. The increasing complexity of linear recurrence sequences. Filter generators. Combining generators. Linear shift register compositions. Schemes with dynamic change of the law of recursion. Schemes with memory elements. Methods of analysis of stream ciphers.
8. Security management. Standards, security audit. Features of speech signals. Scrambling. Frequency signal conversions. Temporary signal conversions. Resistance of temporary permutation systems. Digital Telephony Systems.
9. Public Key Encryption Systems. RSA encryption system. Al-Gamal encryption system. McElice Cipher System. Encryption systems based on the "backpack problem."
10. Identification. Rules for compiling passwords. The complexity of the password verification procedure. “Salted” passwords. Passphrases. Attacks on fixed passwords. Password reuse. Total password guessing. Dictionary attacks. Personal identification numbers. One-time passwords. “Request-response” (strong identification). “Request-response” with using symmetric encryption algorithms. "Request-response" using asymmetric encryption algorithms. Zero-disclosure protocols. Attacks on authentication protocols.
11. Cryptographic hash functions. Hash functions and data integrity. Key hash functions. Keyless hash functions. Data integrity and message authentication. Possible attacks on hash functions.
12. Digital signatures. General Provisions Digital signatures based on public key cryptosystems. Digital signature of Fiat Shamir. Digital Signature of El Gamal. Disposable digital signatures.
13. Key distribution protocols. Key transfer using symmetric encryption. Bilateral protocols. Tripartite Protocols. Key transfer using asymmetric encryption. Protocols without the use of digital signatures. Protocols using digital signature. Public Key Certificates. Open key distribution. Pre-distribution of keys. Schemes of preliminary distribution of keys in a communication network. Secret sharing schemes. Methods for establishing keys for conferencing. Possible attacks on key distribution protocols.
14. Key management. The life cycle of keys. Services provided by a trusted third party. Setting time stamps. Notarization of digital signatures.

15. Some practical aspects of using cipher systems. Message flow analysis. Operator errors. Physical and organizational measures when using cipher systems. Quantum-cryptographic protocol of open key distribution. Quantum channel and its properties. Key distribution protocol.

References

Basic:

1. Акритас А. Основы компьютерной алгебры с приложениями. М.: Мир, 1994.
2. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии. М.: Гелиос АРВ, 2002. 2-е изд.
3. Берлекэмп Э. Алгебраическая теория кодирования. М.: Мир, 1971.
4. Василенко О.Н. Современные способы проверки простоты чисел. Обзор // Кибернетич. сборн. 1988. Вып. 25. С. 162-188.
5. Гашков С. Б. Упрощенное обоснование вероятностного теста Миллера-Рабина для проверки простоты чисел // Дискретная математика. 1998. Т. 10 (4). С. 35—38.
6. Дэвенпорт Дж., Сирэ И., Турнье Э. Компьютерная алгебра. М.: Мир, 1991.
7. Кнут Д. Искусство программирования. Т. 2. Получисленные алгоритмы. Вильямс: М. – СПб. – Киев, 2000. 3-е издание.
8. Кострикин А.И. Введение в алгебру. М.: Наука, 1977.
9. Нечаев В.И. Элементы криптографии. М.: Высшая школа, 1999.
10. Ноден П., Китте К. Алгебраическая алгоритмика. М.: Мир, 1999.
11. Панкратьев Е.В. Компьютерная алгебра. Факторизация многочленов. М.: Изд-во МГУ, 1988.

Additional:

1. Анохин М.И., Варновский Н.П., Сидельников В.М., Ященко В.В. Криптография в банковском деле. М.: МИФИ, 1997.
2. Виноградов И.М. Основы теории чисел. М.: Наука, 1972.
3. Гантмахер Ф. Р. Теория матриц. М., 1954.
4. Касселс Дж. Введение в геометрию чисел. М.: Мир, 1965.
5. Ленг С. Введение в теорию диофантовых приближений. М.: Мир, 1970.
6. Ленг С. Эллиптические функции. М.: Наука, 1984.
7. Чебышев П.Л. Полное собрание сочинений. Т. 1. Теория чисел. Изд-во АН СССР, 1946.
8. Чистов А.Л. Алгоритм полиномиальной сложности для разложения многочленов и нахождения компонент многообразия в субэкспоненциальное время // Зап. науч. семин. ЛОМИ АН СССР. 1984. №137. с. 124-188.

Discipline "Elements of information security"

1. Computer system (CS). Basic concepts. Electronic Document (ED). Types of information in the CS.
2. Vulnerability of computer systems. The concept of access, subject and object of access. The concept of unauthorized access (UAA). Classes and types of UAA.
3. Security policy in computer systems. The concept of security policy and its basic basic concepts. Security rating.
4. Identification of users of CS subjects of data access. User identification task. The concept of an authentication protocol. The concept of identifying information
5. Means and methods of restricting access to files. The main approaches to protecting data from unauthorized access. Ways of fixing access facts. Access logs.
6. Access to data by the process. Features of data protection from change. Reliability of access control systems. An approach based on the formation of a hash function, construction requirements, and implementation methods.
7. Software and hardware encryption. Building hardware and software encryption systems. Designing cryptographic conversion modules based on signal processors.

8. Methods and means of restricting access to computer components. PC components. Classification of protected components of the PC: alienable and inalienable components of the PC.

9. Protecting programs from unauthorized copying. Approaches to the task of copy protection. Binding software to the hardware environment and physical media as the only means of protection against copying software.

10. Storing key information. Passwords and keys. Secret information used for access control: keys and passwords.

11. Management of cryptographic keys. Key Generation. Key distribution.

12. Key distribution authentication protocol for symmetric cryptosystems. Basic concepts and definitions, types of cryptographic protocols, examples.

13. Protocol for asymmetric cryptosystems using public key certificates.

14. Key storage organization (with implementation examples). Direct access magnetic disks. Magnetic and intelligent. TouchMemory Tool

15. Protecting programs from learning. Learning and reverse engineering software. Goals and objectives of studying the work of software. Ways to study software: static and dynamic learning.

REFERENCES

Basic:

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тесты на языке Си. – М.: ТРИУМФ, 2003. – 816 с.

2. Соколов А.В., Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах. – М.: ДМК Пресс, 2002. – 656 с. – (Сер. “Администрирование и защита”).

3. Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии. М.: Гелиос АРВ, 2005.

4. Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. М.: КУДИЦ-ОБРАЗ, 2003.

5. Столлингс В. Операционные системы. М.: Издательский дом «Вильямс», 2014. – 848 с.

Additional:

1. Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд. – М.: Вильямс, 2001. – 672 с.

2. Нечаев В.И. Элементы криптографии (Основы теории защиты информации) / Под ред. В.А. Садовничего. – М.: Высшая школа, 1999. – 109 с.

3. Зубов А.Ю. Криптографические методы защиты информации. Совершенные шифры. М.: Гелиос АРВ, 2005.

4. Фороузан Б.А. Криптография и безопасность сетей: Учебное пособие / Фороузан Б.А.; перевод с англ. под ред. А.Н. Берлина. – М.: Интернет-Университет Информационных технологий: БИНОМ. Лаборатория знаний, 2010 – 784 с.

EXAM RESULTS EVALUATION SCALE

The applicant’s response is assessed as “excellent” when he demonstrates a complete understanding of the principles of organizing information security systems, the ability to use methods and means of protecting computer information, elements of information protection tools, an understanding of the main achievements and development trends of modern IT technologies in the field of information protection, pedagogical and scientific activity. The applicant must be able to clearly, clearly and logically express their thoughts in writing and speaking; be able to apply the acquired knowledge to the solution of practical problems; to reason and draw logical conclusions.

The applicant’s response is assessed as “good” when he demonstrates a significant understanding of the principles of organizing information security systems, the ability to use

methods and means of protecting computer information, elements of information protection tools, an understanding of the main achievements and development trends of modern IT technologies in the field of information protection, pedagogical and scientific activity. The entrant must be able to clearly, clearly and logically express his thoughts in writing and spoken language; be able to apply the acquired knowledge to the solution of practical problems; to reason and draw logical conclusions.

The response of the applicant is assessed as "satisfactory" when the answer indicates a limited understanding of the principles of organizing information security systems, the ability to use methods and means of protecting computer information, elements of information protection, a limited understanding of the main achievements and development trends of modern IT technologies in the field of information protection; technologies of pedagogical and scientific activity. Does not know how to clearly, clearly and logically express his thoughts in writing and speaking; knows how to apply the acquired knowledge to solving practical problems; the ability to reason and draw logical conclusions.

The response of the applicant is assessed as "unsatisfactory" when the answer indicates a complete lack of understanding of the principles of organizing information security systems, the ability to use methods and means of protecting computer information, elements of information protection, lack of understanding of the main achievements and development trends of modern IT technologies in areas of information security, technology, pedagogical and scientific activities. Does not know how to clearly, clearly and logically express his thoughts in writing and speaking; Does not know how to apply the acquired knowledge to solving practical problems; inability to reason and draw logical conclusions.