APPROVED
at a meeting of the Scientific Council
NJSC «Al-Farabi KazNU».
Minutes № ___ dated _____ .

The program of the entrance exam for applicants to the PhD for the group of educational programs
D195 – «Cryptology»

I. General provisions

1. The program was drawn up in accordance with the Order of the Minister of Education and Science of the Republic of Kazakhstan dated October 31, 2018 No. 600 "On Approval of the Model Rules for Admission to Education in Educational Organizations Implementing Educational Programs of Higher and Postgraduate Education" (hereinafter referred to as the Model Rules).

2. The entrance exam for doctoral studies consists of writing an essay, an exam in the profile of a group of educational programs and an interview.

Block	Points
1. Interview	30
2. Essay	20
3. Exam according to the profile of the group of the educational program	50
Total admission score	100/75

3. The duration of the entrance exam is 3 hours 10 minutes, during which the applicant writes an essay and answers an electronic examination. The interview is conducted on the basis of the university before the entrance exam.

II. Procedure for the entrance examination

1. Applicants for doctoral studies in the group of educational programs D195 – «Cryptology» write a problem / thematic essay. The volume of the essay is at least 250 words.

The purpose of the essay is to determine the level of analytical and creative abilities expressed in the ability to build their own argumentation on the basis of theoretical knowledge, social and personal experience.

Types of essays:

- motivational essay with disclosure of motivations for research activity;
- scientific-analytical essay with justification of the relevance and methodology of the planned research;
- problem/thematic essay reflecting various aspects of scientific knowledge in the subject area.

Essay topics:

1. Features of modern cryptographic algorithms and their role in information security
2. Describe the main threats to modern information systems and the methods of counteraction currently used
3. Explain the essence of the concept of cryptanalysis, methods of cryptanalysis of classical algorithms
4. The role and importance of developing post-quantum cryptographic algorithms
5. The role of statistical analysis in decryption tasks
6. Hash functions as cryptographic primitives
7. Describe the concept and principles of blockchain technology
8. Describe the essence of the work of antivirus programs, their classification
9. How can artificial intelligence technologies be used in information security systems
10. What threats have appeared in the software and hardware of information security in connection with the processes of globalization

Topics for exam preparation according to the profile of the group of the educational program:

Discipline «Organization of information security systems»

Topic: Cryptanalysis

Subtopics:

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 < F2n ; +,* > 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 < F2n ; +,* > 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 < F16 ;

+, * >.

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 < F2n ; +,* >. Primitives of the field < F16 ; +,* >.

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.

Discipline «Methods and means of protecting computer information»

Topic: Models and methods of information encryption

Subtopics:

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.

Discipline «Elements of information security tools»

Topic: Information protection of computer systems.

Subtopics:

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.

III. List of references

Main:

1. Дискретная математика для программистов Хаггарти Р. Изд. Техносфера. М: 2012, 400с.

2. CryptoSchool. Joachim von zur Gathen. Springer; 1st ed. 2015 edition.888 pages;

3. Goutam Paul , Subhamoy Maitra. Publisher.RC4 Stream Cipher and Its Variants (Discrete Mathematics and Its Applications). : CRC Press; 1st edition 2019. 311 pages.

4. С.А.Абрамов Элементы компьютерной алгебры линейных обыкновенных дифференциальных, разностных и q-разностных операторов М: МЦМНО 2012 126с.

5. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии. М.: Гелиос АРВ, 2002. 2-е изд.

6. Кнут Д. Искусство программирования. Т. 2. Получисленные алгоритмы. Вильямс: М. – СПб. – Киев, 2000. 3-е издание.

7. Michael E. Whitman, Herbert J. Mattord. Principles of Information Security. Cengage Learning; 6th edition, 2017, 656 pages

8. Richard E. Smith Elementary Information Security. Jones & Bartlett Learning; 3rd edition, 2019. 708 pages

9. David Kim (Author), Michael G. Solomon. Fundamentals of Information Systems Security. Jones & Bartlett Learning; 3rd edition,2016. 548 pages

10. Е. В. Вострецова, Основы информационной безопасности, Екатеринбург, 2019 г., 208с.

11 Ш.Парасрам, А.Замм, Т.Хериянто, Ш.Али, "Kali Linux. Тестирование на проникновение и безопасность", Питер, 2020 г., 448 с.

12. Alan Grid, "Cybersecurity. Learn Information Technology Security: How To Protect Your Electronic Data From Hacker Attacks While You Are Browsing The Internet With Your Smart Devices, Pc Or Television", Via Etenea LTD, 2020, 126 p.

13. Яворски Питер, «Ловушка для багов. Полевое руководство по веб-хакингу», Питер, 2020 г., 272 с.

14. Шелухин О.И., Сакалема Д.Ж., Филинова А.С., "Обнаружение вторжений в компьютерные сети (сетевые аномалии)", 2018 г., 220 с.

15. В. Ф. Шаньгин, "Информационная безопасность и защита информации", ДМК Пресс, 2017 г., 702 с.

16. А. А. Бирюков, "Информационная безопасность. Защита и нападение", ДМК Пресс, 2017г., 434с.

Additional:

1. Michael E. Whitman, Herbert J. Mattord. Principles of Information Security.Cengage Learning; 6th edition, 2017, 656 pages

2. Richard E. Smith Elementary Information Security. Jones & Bartlett Learning; 3rd edition, 2019. 708 pages

3. 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.

4. Анохин М.И., Варновский Н.П., Сидельников В.М., Ященко В.В. Криптография в банковском деле. М.: МИФИ, 1997.

5. Brij Gupta, Gregorio Martinez Perez, Dharma P. Agrawal, Deepak Gupta. Handbook Of Computer Networks And Cyber Security: Principles And Paradigms. Springer, 2020 – p. 957.

6. Aboul Ella Hassanien, Mohamed Elhoseny. Cybersecurity and Secure Information Systems: Challenges and Solutions in Smart Environments. Advanced Sciences and Technologies for Security Applications. Springer International Publishing, 1st ed., 2019 – p. 320.

7. Виноградов И.М. Основы теории чисел. М.: Наука, 1972.

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

9. Kutub Thakur, Al-Sakib Khan Pathan. Cybersecurity Fundamentals: A Real-World Perspective. CRC Press. 2020 – p. 305

10. RC4 Stream Cipher and Its Variants (Discrete Mathematics and Its Applications). Goutam Paul , Subhamoy Maitra. Publisher : CRC Press; 1st edition 2019. 311 pages

11. С.А.Абрамов Элементы компьютерной алгебры линейных обыкновенных дифференциальных, разностных и q-разностных операторов М: МЦМНО 2012 126с. 12. Нечаев В.И. Элементы криптографии (Основы теории защиты информации) / Под ред. В.А. Садовничего. – М.: Высшая школа, 1999. – 109 с.

13. 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.