APPROVED
at the meeting of the Academic Council of NJSC Al-Farabi Kazakh National University
Protocol №14 dated 16.06.2026

The program of the entrance exam for applicants to the PhD for the group of educational programs D095 – «Information security»

1. 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 the electronic examination ticket. The interview is conducted at the university premises before the entrance exam.

2. Procedure for the entrance examination

1. Applicants for doctoral studies in the group of educational programs D195 - «Cryptology» write a problematic / thematic essay. The volume of the essay is at least 250-300 words.

2. The electronic examination card consists of 3 questions.

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

Discipline «**Information Security Systems Organization**»

Topic: Modern Concepts and Technologies of Information Security

Subtopics:

1. Modern approaches to information security. The concept of Zero Trust Architecture (ZTA). Principles of least privilege and continuous trust verification. Enterprise security architecture in the context of digital transformation. Research problem of trust formalization in Zero Trust Architecture. Context parameters (user, device, behavior, location, session risk, resource sensitivity).
2. A research approach to developing an information security process maturity model based on ISO/IEC 27001, NIST Cybersecurity Framework 2.0, and risk-oriented management principles.
3. Architecture and operational principles of a Security Operations Center (SOC). SIEM, SOAR, and XDR systems for incident detection and response. Scientific challenges in automating incident response using SIEM, SOAR, and XDR technologies. Evaluation of event correlation quality, incident prioritization, and automated decision-making.
4. Cyber risk management. Methodologies for risk identification, analysis, and assessment. Quantitative and qualitative risk assessment methods. Threat modeling. Differences between applied risk assessment and a scientific cyber risk model. A model incorporating assets, threats, vulnerabilities, likelihood, impact, uncertainty, and residual risk. Metrics for evaluating reductions in lateral movement, account compromise, excessive privileges, and unauthorized access risks.
5. Cyber Threat Intelligence (CTI). Sources of cyber threat data. Threat taxonomy. The Cyber Kill Chain model. The MITRE ATT&CK framework and its application in attack analysis. Comparison of MITRE ATT&CK and Cyber Kill Chain as adversary behavior modeling frameworks.
6. Methods for detecting cyberattacks. Signature-based, heuristic, and intelligent threat detection methods. IDS, IPS, NDR, and EDR systems. Methodology for evaluating attack detection performance considering false positives, false negatives, class imbalance, latency, and error costs.
7. Machine learning methods in information security. Anomaly detection in network traffic. Attack classification using artificial intelligence techniques. Research challenges related to the generalization capability of machine learning models for network attack detection. The impact of dataset shift, concept drift, class imbalance, and outdated datasets on the reliability of results.
8. Deep learning in cybersecurity systems. Scientific challenges associated with the application of Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Long Short-Term Memory networks (LSTM), Gated Recurrent Units (GRU), and Transformer-based models for intrusion detection and malware analysis.
9. Regulatory and legal framework of the Republic of Kazakhstan. Overview of the Law of the Republic of Kazakhstan “On Access to Information.” Restrictions on the rights of citizens who have or previously had access to state secrets of the Republic of Kazakhstan. Articles of the Criminal Code of the Republic of Kazakhstan related to personal data protection. Competencies of the Government of the Republic of Kazakhstan in the field of personal data protection.

10. Methods for detecting audio-visual deepfakes. Architectures of generative models. Synthetic content detection methods. Assessment of multimedia data authenticity. Audio-visual deepfake detection as a technical and methodological challenge of trust in digital data. A protocol for evaluating the robustness of deepfake detectors against new generative models, compression, noise, and unseen datasets.

11. Cloud security. IaaS, PaaS, and SaaS service models. The Shared Responsibility Model concept. Security management of cloud infrastructures. A model for cyber risk allocation between cloud providers and cloud tenants in IaaS, PaaS, and SaaS environments. Limitations of the Shared Responsibility Model in multi-cloud and hybrid-cloud environments.

12. Security of containerized and microservice-based applications. Docker and Kubernetes technologies. Protection of cloud-native applications. Analysis of data from open sources and active attack vectors when access to restricted sources is obtained. Scientific assessment of software supply chain risks in containerized applications. Vulnerabilities related to container images, registries, CI/CD pipelines, dependencies, SBOMs, artifact signing, and admission control policies.

13. Security of the Internet of Things (IoT) and Industrial Internet of Things (IIoT). Vulnerabilities of distributed devices. Methods for protecting cyber-physical systems. Emerging scientific challenges in designing information security architectures under conditions of digital transformation, remote work, SaaS services, cloud computing, mobile devices, and IoT.

14. Cyberattack attribution. Methods for identifying attack sources. The use of Threat Intelligence, OSINT, and behavioral analysis for attribution. Epistemological and methodological limitations of cyberattack attribution. Incomplete data, false flag operations, TTP reuse, publicly available tools, OSINT sources, and confidence levels.

15. Emerging directions in information security. Autonomous defense systems. Cyber resilience. Artificial intelligence in incident response decision-support systems. Scientific challenges of applying artificial intelligence to automated incident response.

Discipline **«Elements of Information Protection Tools»**

Topic: Protection of Information in Computer Systems

Subtopics:

1. Architecture of modern computer systems. Computing system models (local, distributed, cloud-based). Data flows in computer systems. Fundamental principles of information security within system architectures.

2. Threat modeling in computer systems. Classification of threats: internal and external, intentional and accidental. Information leakage channels. Attacker model and capabilities. Information security risk assessment.

3. Access control mechanisms in modern operating systems. Discretionary and mandatory access control models. Role-Based Access Control (RBAC). Attribute-Based Access Control (ABAC).

4. Modern methods of user identification and authentication. Biometric technologies, multi-factor authentication, and hardware tokens. Authentication protocols in distributed systems.

5. Security logging and monitoring systems. Security event logging and access log analysis. SIEM systems and event correlation. Detection of anomalous activities.

6. Data integrity in computer systems. Methods for integrity monitoring of files and processes. Checksums, hashing, and digital signatures. Real-time protection against unauthorized data modification.

7. Hardware and software information protection tools. Trusted Platform Module (TPM) architecture. Hardware Security Modules (HSM). Integration of cryptographic functions into hardware.

8. Protection of computer hardware components. Classification of protected resources: processors, memory, and peripheral devices. Methods for preventing physical access and hardware attacks.

9. Protection of software against unauthorized copying. Software licensing. Hardware protection keys. Binding software to hardware platforms and digital identifiers.

10. Secret management in computer systems. Storage of passwords and cryptographic keys. Secure storage solutions (Key Vault, Secure Enclave). Secret management policies.

11. Cryptographic key lifecycle management. Key generation, distribution, storage, rotation, and destruction. Centralized and decentralized key management models (KMS).

12. Symmetric authentication and key distribution protocols. Kerberos as an example of a centralized authentication system. Trusted Key Distribution Center (KDC) mechanisms.

13. Asymmetric authentication protocols. Public Key Infrastructure (PKI). Certificate validation, chains of trust, and certificate revocation mechanisms (CRL, OCSP).

14. Organization of storage and protection of key information. Hardware and software key carriers. Smart cards, security tokens, and TPM modules. Methods of protecting keys from extraction and duplication.

15. Reverse engineering and software protection against analysis. Static and dynamic program analysis methods. Code obfuscation, anti-debugging mechanisms, and protection against disassembly and reverse engineering.

Discipline **«Methods and Tools for Computer Information Protection»**

Topic: Cryptanalysis.

Subtopics:

1. Classical ciphers and their cryptanalysis. Caesar and affine ciphers, decryption and brute-force attacks. Frequency analysis of substitution ciphers. Weaknesses of classical ciphers and frequency analysis of texts in Kazakh and Russian languages.

2. The ring of integers, Euclidean algorithm, and its consequences. Representation of the greatest common divisor. Theory of congruences. Properties of congruences modulo a given number. Invertible elements modulo n.

3. Euler’s totient function and its properties. Euler’s function for prime numbers. Multiplicative property of Euler’s function. Formula for calculating Euler’s function values. Exponentiation using Euler’s theorem.

4. Fermat–Euler theorem and the fundamental theorem underlying the RSA cryptosystem.

5. RSA cryptosystem: encryption and decryption processes, mathematical justification. Encryption of a given plaintext using a public key. Decryption using a private key.

6. RSA digital signature: concept and mathematical foundation.

7. Implementation of RSA digital signatures: document signing procedure.

8. Implementation of RSA digital signatures: signature verification using a public key.

9. Distribution of prime numbers in the set of natural numbers and security evaluation of the RSA cryptosystem.

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

11. Construction of the field $<F_{2^n}; +, *>$ as a field of residues modulo an irreducible polynomial. Definition of addition and multiplication in the field. Additive and multiplicative inverses of nonzero elements. Construction of the field $<F_{16}; +, *>$.

12. Lagrange's theorem on divisibility of subgroup order by group order. Consequences concerning the order of an element. Examples of subgroups of Zn. Primitive element theorem for the field $<F_{2^n}; +, *>$. Primitive elements of the field $<F_{16}; +, *>$.

13. Construction of a field based on n-bit binary blocks. Definition of addition and multiplication operations. Additive and multiplicative inverses of nonzero elements. Primitive elements of the field. Construction of a field of 4-bit binary blocks and identification of its primitive elements.

14. Diffie–Hellman problem. Establishing a shared secret between remote users based on the computational hardness of the Diffie–Hellman problem. Solving the key exchange problem for remote users.

15. ElGamal cryptosystem. Key exchange process, encryption, and decryption procedures. Practical implementation using an example.

3. List of references

1. Stallings W. *Cryptography and Network Security: Principles and Practice*. — 8th ed. — Pearson, 2020. — 768 p.

2. Katz J., Lindell Y. *Introduction to Modern Cryptography*. — 2nd ed. — CRC Press, 2014. — 538 p.

3. Menezes A., van Oorschot P., Vanstone S. *Handbook of Applied Cryptography*. — CRC Press, 1996. — 816 p.

4. Schneier B. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. — 2nd ed. — Wiley, 1996. — 784 p.

5. Ferguson N., Schneier B., Kohno T. *Cryptography Engineering*. — Wiley, 2010. — 384 p.

6. Paar C., Pelzl J. *Understanding Cryptography*. — Springer, 2010. — 372 p.

7. Koblitz N. *A Course in Number Theory and Cryptography*. — Springer, 1994. — 236 p.

8. Diffie W., Hellman M. New Directions in Cryptography // *IEEE Transactions on Information Theory*. — 1976. — Vol. 22(6). — P. 644–654.

9. Rivest R., Shamir A., Adleman L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems // *Communications of the ACM*. — 1978. — Vol. 21(2). — P. 120–126.

10. ElGamal T. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms // *IEEE Transactions on Information Theory*. — 1985. — Vol. 31(4). — P. 469–472.

11. Shannon C. E. Communication Theory of Secrecy Systems // *Bell System Technical Journal*. — 1949. — Vol. 28. — P. 656–715.

12. Bishop M. *Computer Security: Art and Science*. — Addison-Wesley, 2003. — 1134 p.

13. Pfleeger C., Pfleeger S. L. *Security in Computing*. — 5th ed. — Pearson, 2015. — 624 p.

14. Anderson R. *Security Engineering*. — 3rd ed. — Wiley, 2020. — 1250 p.

15. Easttom C. *Modern Cryptography: Applied Mathematics for Encryption and Information Security*. — McGraw-Hill, 2021. — 600 p.

16. ISO/IEC 27001:2022. *Information Security Management Systems — Requirements*. — International Organization for Standardization, 2022.

17. ISO/IEC 27002:2022. *Information security, cybersecurity and privacy protection — Information security controls*. — ISO, 2022.

18. Фомичев В. М. *Дискретная математика и криптография*. — М.: Диалог-МИФИ, 2012. — 400 с.

19. Ященко В. В. *Введение в криптографию*. — М.: МЦНМО, 2000. — 272 с.

20. Ожигов Ю. И. *Основы защиты информации в компьютерных системах*. — М.: Горячая линия-Телеком, 2018. — 320 с.