Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Петренко Вячеслав Иванович
Должность: и.о. директора Института цифрового развития
Дата подписания: 03.07.2023 10:22:36
Уникальный программный ключ:
b47f96eea65a16e179f94dbf7fb0b10000e

# Discipline annotation

| Discipline name | **Методы и средства криптографической защиты информации / Methods and means of information cryptographic protection** |
|---|---|
| Summary | Basic concepts of cryptography. The simplest substitution and permutation ciphers. Block ciphers. DES American encryption standard. Practical application of the American standard. AES cryptographic security standard. How the AES encryption algorithm works. Magma data encryption standard. Domestic encryption standard “Kuznechik” (Grasshopper). Synchronous Stream Encryption Systems. Self-synchronizing stream encryption systems. Software implementations of ciphers. Modes of using block ciphers. Encryption modes with feedback. Reliability of ciphers. Strength of ciphers. Asymmetric encryption systems. Practical implementation of asymmetric encryption systems. Electronic digital signature. Practical implementation of electronic digital signatures. Key management. Key distribution protocols. Cryptographic secret sharing schemes. Authentication protocols. Zero knowledge authentication protocols and their applications. Hidden channel. Construction principles. Cryptographic hash functions. |
| Learning outcomes of the discipline | - effectively applies knowledge of the theory and methodology of the course when solving computer crimes, when working with confidential information and state secrets, when working with organizational and legal support, when working with ES, when protecting copyright and international law, when conducting examinations of crimes in the field of computer information; applies regulatory legal acts in the protection of information; evaluates the state of organizational information protection at the facility.<br>- understands basic principles of creating means of cryptographic and technical protection of information to solve professional tasks.<br>- applies means of cryptographic and technical protection of information to solve professional tasks.<br>- chooses the best option of using the skills and methods of applying means of cryptographic and technical protection of information to solve professional tasks |
| Workload, c. u. | 8c. u. |
| Reporting Forms | Graded test- 5th semester<br>Exam- 6th semester |
| **List of essential and supplementary literature necessary for mastering the discipline** | |
| Essential literature | 1. Basalova, G. V. Fundamentals of cryptography: textbook / Basalova G. V. - Moscow: Internet University of Information Technologies (INTUIT), 2016. - 282 p. - The book is in the basic version of IPRbooks ELS<br>2. Kukina, E. G. Introduction to cryptography: Collection of tasks and exercises / Kukina E. G. - Omsk: Omsk State University named after F. M. Dostoevsky, 2013. - 91 p. - The book is in the basic version of IPRbooks ELS. - ISBN 978-5-7779-1588-7 |
| Supplementary literature | 1. The use of artificial neural networks and the system of residual classes in cryptography / [authours board: Chervyakov N. I., Evdokimov A. A., and others]. - Moscow: FIZMATLIT, 2012. - 280 p.: ill. - App.: p. 269-279. - Bibliography: p. 269-279 (191 titles) and at the end of ch. - ISBN 978-5-9221-1386-1. |