

Discipline annotation

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Петренко Вячеслав Иванович

Должность: директор Института цифровых технологий

Дата подписания: 28.03.2024 14:31:33

Уникальный программный ключ:

b47f96eea65a16e179f94dbf7fb0b10000e7ad4d

Discipline name	Protection of critical information infrastructure objects
Summary	<p>Essential concepts and definitions of the studied discipline. Legal basis for ensuring the security of critical information infrastructure (CII) of the Russian Federation. State system for detecting, preventing and eliminating the consequences of computer attacks on information resources of the Russian Federation. Organizational and legal basis for certification of significant CII objects, licensing of activities in the field of information security. System of certification of information protection means. Threats to the security of information processed by CII objects. Sources of information security threats. Vulnerabilities of CII objects, classification of vulnerabilities. Ways of realization of information security threats and their consequences. Information Security Threat Databank The structure of a model of threats to the information security of a significant CII object. Categorization of CII objects. Register of significant CII objects. List of indicators of criteria for the significance of CII objects of the Russian Federation and their significance. Requirements to ensure the safety of significant CII objects. Requirements for software and hardware used to ensure the safety of significant CII objects. Requirements for protection classes of information security tools and computer equipment for various categories of significance of CII objects. Security system of a significant CII object. Stages (steps) of work to create security systems for a significant CII object. Control over ensuring the safety of a significant CII object.</p>
Learning outcomes of the discipline	<ul style="list-style-type: none"> - determines the categories of significance of CII objects; - determines the requirements for ensuring the safety of a significant CII object; - develops models of threats to the information security of significant CII objects; - justifies organizational and technical measures to be implemented within the security system of a significant CII object; - develops the architecture of the security system of a significant CII object; - selects information security means taking into account the category of significance of the CII object; - determines requirements for software and hardware settings.
Workload, c. u.	3 c. u.
Reporting Forms	Graded credit – 5 semester
List of essential and supplementary literature necessary for mastering the discipline	
Essential literature	<ol style="list-style-type: none"> 1. Novikov V. K. Organizational and legal support of information security: Study guide. In 2 parts. Part 1. Legal support of information security. - M.: MIET, 2013. - 184 p. 2. Novikov V. K. Organizational and legal support of information security: Study guide. In 2 parts. Part 2. Organizational support of information security. - M.: MIET, 2013. - 172 p. 3. Melnikov, V. V. Information security in automated systems. - M.: Finansy i statistika, 2003. – 368 p. 4. Software and hardware for information security. Program and data protection: textbook for universities. - M.: Radio i svyaz, 2000. – 168 p.
Supplementary literature:	<ol style="list-style-type: none"> 1. Federal Law of July 26, 2017 No. 187-FZ “On the security of critical information infrastructure of the Russian Federation.”

- | | |
|--|---|
| | <ol style="list-style-type: none">2. Federal Law of July 26, 2017 No. 193-FZ “On amendments to certain RF legislative acts in view of the adoption of the Federal Law “On the security of CII of the RF”.3. Decree of the President of the Russian Federation dated March 30, 2022 No. 166 “On measures to ensure the technological independence and security of the RF CII.”4. Rules for the implementation of state control in the field of ensuring the security of significant objects of critical information infrastructure of the Russian Federation. Approved by Decree of the Government of the Russian Federation of February 17, 2018 No. 162.5. On approval of the Rules for the categorization of critical information infrastructure objects of the Russian Federation, as well as a list of indicators of criteria for the significance of critical information infrastructure objects of the Russian Federation and their values. Approved by Decree of the Government of the Russian Federation of February 8, 2018 No. 127 (as amended on December 20, 2022).6. The procedure for maintaining a Register of significant objects of critical information infrastructure of the Russian Federation. Approved by order of the FSTEC of Russia dated December 6, 2017 No. 227.7. Requirements for the creation of security systems for significant objects of critical information infrastructure of the Russian Federation and ensuring their operation. Approved by order of the FSTEC of Russia dated December 21, 2017 No. 235.8. Requirements for ensuring the security of significant objects of critical information infrastructure of the Russian Federation. Approved by order of the FSTEC of Russia dated December 25, 2017 No. 239 (as amended by order of the FSTEC of Russia dated August 9, 2018 No. 138).9. Methodological document. Methodology for assessing threats to information security. Approved by the FSTEC of Russia on February 5, 2021. |
|--|---|