

Документ подписан простой электронной подписью
 Информация о владельце:
 ФИО: Петренко Вячеслав Иванович
 Должность: и.о. директора Института цифрового развития
 Дата подписания: 28.03.2024 14:31:33
 Уникальный программный ключ:

Discipline annotation

Discipline name Summary	Персональная кибербезопасность / Personal Cybersecurity
	Cyber security: world of specialists and criminals. Cyber security cube. Properties of countering cybersecurity threats. Cyber security threats, vulnerabilities and attacks. Ways to protect restricted access information. Ways to ensure data integrity. The concept of "five nines". Protection of cyber security levels. Cyber security specialists
Learning outcomes of the discipline	- forms the goals, priorities, duties and powers of the personnel serving the facilities and CMTN, the means and systems for their protection against unauthorized access; distributes the duties and powers of the personnel, the service facilities and CMTN, the means and systems for their protection against unauthorized access; checks the level of qualification of the personnel serving the facilities and CMTN, means and systems for their protection against unauthorized access, including when hiring; - sets tasks for the personnel to ensure the protection of the CMTN against unauthorized access and organizes their implementation; organizes control over the implementation of organizational and technical measures to ensure the protection of the CMTN against unauthorized access; organizes the redistribution of duties and powers of personnel serving the facilities and CMTN, means and systems for their protection against unauthorized access; - has mastered the goals and objectives of personnel management, service facilities and CMTN, means and systems for their protection against unauthorized access; has mastered the methodology for choosing and organizing management decisions to ensure the protection of telecommunication networks against unauthorized access; uses the guidance and methodological documents of the authorized federal executive authorities for information protection - determines the composition of software and hardware for information protection in computer networks; develops the procedure for using software and hardware for information protection in computer networks; generates configuration templates for software and hardware for information protection in computer networks; - evaluates threats to information security in computer networks; sets up packet filtering rules in computer networks; justifies the choice of used software and hardware to protect information in computer networks; - understands the principles of building computer networks; understands the operation of the network protocol stack of operating systems; understands the principles of building computer networks; understands the operation of the network equipment protocol stack - determines the procedure for installing software in order to comply with information protection requirements; monitors compliance with information protection requirements when installing software, including anti-virus software; formulates requirements for the parameters of anti-virus protection for the

	correct operation of the software; - analyzes threats to the security of software information; formulates rules for the safe operation of software; justifies the rules for the safe operation of software; - understands the architecture of information protection subsystems in operating systems; understands the principles of building database management systems; understands the main tools and methods for analyzing software implementations
Workload, c. u.	2 c. u.
Reporting Forms	Credit – 1st semester
List of essential and supplementary literature necessary for mastering the discipline	
Essential literature	1. Network protection based on CiscoSystems technologies. Practical course [Electronic source]: study guide / A. N. Andronchik [et al.]. — Electronic text data. - Yekaterinburg: Ural Federal University, 2014. - 180 p. — 978-5-7996-1201-6. — Available at: http://www.iprbookshop.ru/65983.html 2. Shangin V. F. Information security and information protection [Electronic source] / V. F. Shangin. — Electronic text data. - Saratov: Vocational education, 2017. - 702 p. — 978-5-4488-0070-2. - Available at: http://www.iprbookshop.ru/63594.html
Supplementary literature	1. Melnikov, V. P., Kleimenov, S. A., Petrakov, A. M. Information security and protection of information: textbook for university students; ed. by S. A. Kleymenova. - 5th ed., reprint. - M.: Academia, 2011. - 332 p. - (Higher professional education. Informatics and computer technology). - Bibliography: p. 327-328. - ISBN 978-5-7695-7738-3. 2. Osipenko A. L. Network computer crime. Theory and practice of struggle [Electronic source]: monograph / A. L. Osipenko. — Electronic text data. - Omsk: Omsk Academy of the Ministry of Internal Affairs of Russia, 2009. - 480 p. — 978-5-88651-445-2. - Available at: http://www.iprbookshop.ru/36083.html. 3. Prokhorova O. V. Information security and information protection [Electronic source]: textbook / O. V. Prokhorov. — Electronic text data. - Samara: Samara State University of Architecture and Civil Engineering, ASV ELS, 2014. - 113 p. — 978-5-9585-0603-3. — Available at: http://www.iprbookshop.ru/43183.html. 4. Shangin V. F. Protection of computer information. Effective methods and means [Electronic source] / V. F. Shangin. — Electronic text data. - Saratov: Vocational education, 2017. - 544 p. — 978-5-4488-0074-0. — Available at: http://www.iprbookshop.ru/63592.html.