

Документ подписан простой электронной подписью
 Информация о владельце:
 ФИО: Петренко Вячеслав Иванович
 Должность: и.о. директора Института цифрового развития
 Дата подписания: 05.07.2024 09:35:26
 Уникальный программный ключ:
 b47f96eea65a20e279f94abf1bb0b10000e7ad4d

Аннотация дисциплины

Наименование дисциплины	Экспертиза вычислительной техники и компьютерных носителей информации
Содержание	В рамках данной дисциплины изучаются технологии и методы проведения экспертизы компьютерных систем и носителей информации. Особое внимание уделено правилам проведения согласно конституции РФ. Рассмотрены основные программные и технические средства проведения экспертизы компьютерных систем, а также подтверждения подлинности аудио- видео- фото файлов.
Реализуемые компетенции	ОПК-6.2. Способен проводить экспертные исследования вычислительной техники и компьютерных носителей информации в рамках информационно-аналитической и технической экспертизы компьютерных систем. ПК-1. Способен разрабатывать требования по защите информации для формирования политик безопасности компьютерных систем и сетей. ПК-2. Способен проводить анализ безопасности компьютерных систем.
Результаты освоения дисциплины (модуля)	ОПК-6.2 Знать: нормативные и правовые акты, регламентирующие проведение компьютерно-технических экспертиз, современные методы и средства проведения экспертиз вычислительной техники и носителей компьютерной информации, основные типы экспертиз вычислительной техники и носителей компьютерной информации Уметь: обосновывать экспертное заключение в соответствии с требованиями, предъявляемыми к работе привлекаемого эксперта при проведении следственных и судебных действий; обращаться с инструментальными средствами проведения экспертиз вычислительной техники и носителей компьютерной информации; собирать, обрабатывать, анализировать и хранить данные, получаемые в ходе проведения экспертиз вычислительной техники и носителей компьютерной информации. Владеть: правилами и методами проведения экспертиз в соответствии с требованиями, предъявляемыми к работе привлекаемого эксперта при проведении следственных и судебных действий; способами обращения с инструментальными средствами проведения экспертиз вычислительной техники и носителей компьютерной информации; способами и методами сбора, обработки, анализа и хранения данных, получаемых в ходе проведения экспертиз вычислительной техники и носителей компьютерной информации. ПК-1 Знать: принципы построения компьютерных систем и сетей; модели безопасности компьютерных систем; виды политик безопасности компьютерных систем и сетей; принципы построения средств криптографической защиты информации; национальные, межгосударственные и международные стандарты в области защиты информации; возможности используемых и планируемых к использованию средств защиты информации; нормативные

	правовые акты в области защиты информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; организационные меры по защите информации Уметь: анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия; разрабатывать профили защиты компьютерных систем; формулировать задания по безопасности компьютерных систем; выполнять анализ безопасности компьютерных систем и разрабатывать рекомендации по эксплуатации системы защиты информации. Владеть: навыками разработки технических заданий на создание средств защиты информации; классификации информационной системы по требованиям защиты информации. ПК-2 Знать: уязвимости компьютерных систем и сетей; криптографические методы защиты информации; принципы построения систем управления базами данных; средства анализа конфигураций; национальные, межгосударственные и международные стандарты в области защиты информации; нормативные правовые акты в области защиты информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; организационные меры по защите информации Уметь: анализировать компьютерную систему с целью определения уровня защищенности и доверия; прогнозировать возможные пути развития действий нарушителя информационной безопасности; производить анализ политики безопасности на предмет адекватности; проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах; составлять и оформлять аналитический отчет по результатам проведенного анализа; разрабатывать предложения по устранению выявленных уязвимостей. Владеть: навыками определения уровня защищенности и доверия в компьютерных системах; оценки рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем; оценки соответствия механизмов безопасности компьютерной системы требованиям существующих нормативных документов, а также их адекватности существующим рискам; подготовки аналитического отчета по результатам проведенного анализа; формулирования предложений по устранению выявленных уязвимостей.
Трудоемкость, з.е.	5
Форма отчетности	Зачет, 8 семестр
Перечень основной и дополнительной литературы, необходимой для освоения дисциплины	
Основная литература	1. Просис, К. Расследование компьютерных преступлений / Крис Просис, Кевин Мандиа; [пер. с англ. О. Труфанов]. – М.: Лори, 2013. – 476 с.: ил.d23. – ISBN 978-5-85582-314-1 Современные компьютерные технологии Электронный ресурс:

	Учебное пособие / Р. Г. Хисматов [и др.]. – Казань: Казанский национальный исследовательский технологический университет, 2014. – 83 с. – Книга находится в премиум-версии ЭБС IPR BOOKS. – ISBN 978-5-7882-1559-4
Дополнительная литература	1. Digital Forensics and Incident Response. Gerard Johansen. 2017. 2. Acharyulum, G.V.R.K. (2011), Information Management in a Health Care System: Knowledge Management Perspective. International Journal of Innovation, Management and Technology, Vol. 2(6), 534-537. 3. Biros, David P., Mark Weiser and John Witfield. (2007). Managing digital forensic knowledge an applied approach. Proceedings of the 5th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia. https://ro.ecu.edu.au/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsedir=1&article=1010&context=adf. 4. Brown, John Seely and Paul Duguid. (1998). Organizing Knowledge. California Management Review, Vol. 40(3), 90-111. 5. Chang, Weiping and Peifang Chung. (2014). Knowledge Management in Cybercrime Investigation – A Case Study of Identifying Cybercrime Investigation Knowledge in Taiwan. Pacific-Asia Workshop on Intelligence and Security Informatics (PAISI 2014: Intelligence and Security Informatics), pp. 8-17. 6. Chow, Peter. (2012). Surfing the Web Anonymously – The Good and Evil of the Anonymizer. SANS Institute InfoSec Reading Room. https://www.sans.org/reading-room/whitepapers/detection/surfing-webanonymously-good-evil-anonymizer-33995. Citizen Lab (n.d.). Research. https://citizenlab.ca/category/research/. 7. Cybercrime Centres of Excellence Network for Training, Research and Education (n.d.). 2Centre.http://www.2centre.eu/.