

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Петренко Вячеслав Иванович
Должность: и.о. директора Института цифрового развития
Дата подписания: 04.09.2023 12:47:21
Уникальный программный ключ:
b47f96eea65a18c1391248077b00b10000e7ad4d

Аннотация дисциплины

Наименование дисциплины	Основы компьютерной криминалистики
Краткое содержание	Цифровая криминалистика и её значение для расследования компьютерных преступлений и инцидентов. Основы цифровой криминалистики и цифровой судебной экспертизы. Способы и методы реагирования на инциденты. Нормативные и правовые акты, регламентирующие деятельность эксперта по компьютерной криминалистике. Методики сбора и анализа цифровых доказательств. Методы и технологии криминалистической визуализации при расследовании компьютерных преступлений и инцидентов. Основы анализа вредоносного ПО, цифровых угроз и возможного предупреждения компьютерных преступлений и инцидентов.
Результаты освоения дисциплины (модуля)	Применяет нормативные правовые акты, методические документы, основы компьютерной криминалистики при проведении следственных и судебных действий по информационно-аналитической и технической экспертизе компьютерных систем. Подготавливает экспертные заключения по результатам выполненных работ по информационно-аналитической и технической экспертизе компьютерных систем.
Трудоемкость, з.е.	10
Формы отчетности	Зачет с оценкой; Экзамен
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 2. 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/.
--	---