

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:
b47f96eea65a20e275f94bbf7bb0b10000e7ad4d

Аннотация дисциплины

Наименование дисциплины	Основы компьютерной криминалистики
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.
Реализуемые компетенции	ОПК-6.3. Способен в качестве привлекаемого эксперта при проведении следственных и судебных действий применять нормативные правовые акты, методические документы, основы компьютерной криминалистики. ПК-8. Способен устранять сбои и отказы сетевых устройств и операционных систем.
Результаты освоения дисциплины (модуля)	ОПК-6.3 Знать: порядок проведения экспертизы вычислительной техники и носителей компьютерной информации с учетом нормативных правовых актов; виды преступлений в сфере компьютерной информации; основные требования, предъявляемые к составу и оформлению научно-технических экспертных заключений по результатам выполненных работ по информационно-аналитической и технической экспертизе компьютерных систем; методику проведения работ по информационно-аналитической и технической экспертизе компьютерных систем. Уметь: подготавливать научно-технические экспертные заключения, по результатам выполненных работ по информационно-аналитической и технической экспертизе компьютерных систем; обобщать и анализировать данные, получаемые в ходе проведения работ по информационно-аналитической и технической экспертизе компьютерных систем; фиксировать и документировать следы компьютерных преступлений, правонарушений и инцидентов. Владеть: способами подготовки научно-технических экспертных заключений, по результатам выполненных работ по информационно-аналитической и технической экспертизе компьютерных систем; методами обобщения и анализа данных, получаемых в ходе проведения работ по информационно-аналитической и технической экспертизе компьютерных систем; способами фиксации и документирования следов компьютерных преступлений, правонарушений и инцидентов. ПК-8 Знать: общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети; архитектуру аппаратных, программных и программно-аппаратных средств администрируемой сети;

	<p>инструкции по установке администрируемых сетевых устройств; инструкции по эксплуатации администрируемых сетевых устройств; инструкции по установке администрируемого программного обеспечения; инструкции по эксплуатации администрируемого программного обеспечения; протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем; модель ISO для управления сетевым трафиком; модели IEEE; регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе; требования охраны труда при работе с сетевой аппаратурой администрируемой сети.</p> <p>Уметь: анализировать сообщения об ошибках в сетевых устройствах и операционных системах; локализовать отказ и инициировать корректирующие действия; пользоваться нормативно-технической документацией в области инфокоммуникационных технологий.</p> <p>Владеть: навыками выявления сбоев и отказов сетевых устройств и операционных систем; определения сбоев и отказов сетевых устройств и операционных систем; устранения последствий сбоев и отказов сетевых устройств и операционных систем; сопоставления аварийной информации от различных устройств сети; локализации отказов в сетевых устройствах и операционных системах; инициирования корректирующих действий; регистрации сообщений об ошибках в сетевых устройствах и операционных системах; фильтрации сообщений об ошибках в сетевых устройствах и операционных системах; маршрутизации сообщений об ошибках в сетевых устройствах и операционных системах.</p>
Трудоемкость, з.е.	12
Форма отчетности	Зачет с оценкой, 9 семестр; экзамен, 10 семестр
Перечень основной и дополнительной литературы, необходимой для освоения дисциплины	
Основная литература	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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.

	<p>4. Brown, John Seely and Paul Duguid. (1998). Organizing Knowledge. California Management Review, Vol. 40(3), 90-111.</p> <p>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.</p> <p>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/.</p> <p>7. Cybercrime Centres of Excellence Network for Training, Research and Education (n.d.). 2Centre. http://www.2centre.eu/.</p>
--	--