

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:
 b47f96ee65a20e275f94bbf7db0b10000e7ad40

Аннотация дисциплины

Наименование дисциплины	Технологии выявления следов компьютерных преступлений, правонарушений и инцидентов
Содержание	В рамках данной дисциплины изучаются технологии расследования компьютерных преступлений и инцидентов. Рассмотрен перечень действий и мер сотрудника информационной безопасности предприятия (организации) при немедленном обнаружении действия компьютерного преступления либо следов его совершения от начала преступления до конца расследования. Терминология и сферы применения компьютерной криминалистики. Принципы работы и ответственность эксперта при проведении исследования. Основной инструментарий эксперта. Выявление взлома и фишинга конечных пользователей. Компьютерные вирусы. Киберпреследование, «кража личности» и способы противодействия данным угрозам. Кибервымогательство, спам и способы противодействия данным угрозам. Выявление фактов, мест и времени неправомерного доступа к информации в компьютерной системе или сети. Формирование методики расследования. Анализ механизма преступной деятельности. Выявление фактов, мест и времени неправомерного доступа к информации в компьютерной системе или сети. Криминалистические особенности выявления и расследования преступного доступа к компьютерной информации. Типичные следственные ситуации и разработка типовых программ расследования в таких ситуациях. Установление надежности средств защиты компьютерной информации. Анализ потенциальных и реальных ситуаций, представляющих угрозу безопасности информации. Ознакомление с инструкциями для должностных лиц, имеющих отношение к защите информации. Перечень пунктов, подлежащих установлению. Выявление авторства вредоносных программ. Технология выявления лиц, причастных к совершению компьютерного преступления. Формирование доказательной базы по компьютерному преступлению.
Реализуемые компетенции	ОПК-6.1. Способен использовать технологии поиска, фиксации и документирования следов компьютерных преступлений, правонарушений и инцидентов. ПК-8. Способен устранять сбои и отказы сетевых устройств и операционных систем.
Результаты освоения дисциплины (модуля)	ОПК-6.1 Знать: основные этапы и методы проведения расследования компьютерных преступлений, правонарушений и инцидентов; методы и средства сбора и обращения с доказательными данными. Уметь: определять причины, цели и условия изменения свойств (состояния) программного обеспечения; обращаться со свободно распространяемыми инструментальными средствами сбора, анализа и хранения доказательных данных. Владеть: инструментальными средствами поиска, 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; 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. 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. 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.
Трудоемкость, з.е.	5
Форма отчетности	Экзамен, 7 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/.
--	---