

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Петренко Вячеслав Иванович
Должность: и.о. директора Института цифрового развития
Дата подписания: 26.09.2022 15:26:55
Уникальный программный ключ:
b47f96a6d65d791948bf7fb0b10000e7ad4d

Аннотация дисциплины

Наименование дисциплины	
Системы управления инцидентами информационной безопасности	
Краткое содержание	Разработка политики менеджмента инцидентов кибербезопасности. Документирование политики менеджмента инцидентов кибербезопасности. Формы и процедуры обнаружения, оповещения, оценки и реагирования на инциденты кибербезопасности. Инструменты обнаружения, оповещения, оценки и реагирования на инциденты кибербезопасности. Обновление политик менеджмента информационной безопасности и рисков. Обнаружение и оповещение о возникновении событий кибербезопасности в ручном режиме. Обнаружение и оповещение о возникновении событий кибербезопасности в автоматизированном режиме. Сбор информации, связанной с событиями кибербезопасности. Правила отнесения событийной информации к инцидентам кибербезопасности. Способы реагирования на инциденты кибербезопасности. Методы расследования инцидентов кибербезопасности. Технологии предупреждения инцидентов кибербезопасности.
Результаты освоения дисциплины (модуля)	Применяет математический аппарат для освоения теоретических основ и практического использования физических методов. Выполняет анализ защищенности компьютерных систем с использованием сканеров безопасности, сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей. Осуществляет поиск уязвимостей и недокументированных возможностей программного обеспечения. Использует формализованные модели, методы и алгоритмы решения типовых задач автоматизированной информационно-аналитической поддержки процессов принятия решений. Оценивает эффективность и качество в задачах прогнозирования, планирования, принятия решений при различной априорной неопределенности имеющейся информации.
Трудоемкость, з.е.	5
Формы отчетности	Экзамен
Перечень основной и дополнительной литературы, необходимой для освоения дисциплины	
Основная литература	1. Нестеров, С.А. Основы информационной безопасности. [Электронный ресурс]: учеб. пособие. Электрон. дан. СПб.: Лань, 2017. 324 с. Режим доступа: http://e.lanbook.com/book/90153 2. Безопасность и управление доступом в информационных системах: Учебное пособие / А.В. Васильков, И.А.Васильков. – М.: Форум: НИЦ ИНФРА-М, 2013. - 368 с.: ил.; 60х90 1/16. – (Профессиональное образование) (переплет) ISBN 978-5-91134-360-6 - http://znanium.com/bookread2.php?book=405313 3. Жукова, М. Н. Управление информационной безопасностью. Ч. 2. Управление инцидентами информационной безопасности [Электронный ресурс]: учеб.пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. – Красноярск:Сиб. гос. аэрокосмич. ун-т, 2012. – http://znanium.com/bookread2.php?book=463061
Дополнительная литература	1. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 416 с.: ил.; 60х90 1/16. – (Профессиональное образование). (переплет) ISBN 978-5-8199-0331-5 - http://znanium.com/bookread2.php?book=423927

	2. Информационная безопасность конструкций ЭВМ и систем: учебное пособие / Е.В. Глинская, Н.В. Чичварин. – М.: НИЦ ИНФРА-М, 2016. - 118 с. URL: http://znanium.com/bookread2.php?book=507334 3. Партыка Т. Л. Информационная безопасность [Электронный ресурс]: Учебное пособие /Т.Л. Партыка, И.И. Попов. – 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2014. – 432 с.: ил.; 60х90 1/16. – (Профессиональное образование). ISBN 978-5-91134-627-0, 1000 экз. http://znanium.com/bookread2.php?book=420047
--	--