

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:
 b47f96eea65a20e275f94ab71bb0b10000e7ad4d

Аннотация дисциплины

Наименование дисциплины	Менеджмент инцидентов кибербезопасности
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
Реализуемые компетенции	ПК-3. Способен проводить сертификацию программно-аппаратных средств защиты информации и анализ результатов. ПК-4. Способен проводить инструментальный анализ защищенности компьютерной системы и осуществлять поиск уязвимостей программного обеспечения. ПК-9. Способен выполнять автоматизированную информационно-аналитическую поддержку процессов принятия решений в профессиональной деятельности.
Результаты освоения дисциплины (модуля)	ПК-3 Знать: национальные, межгосударственные и международные стандарты в области защиты информации; национальные стандарты на проведение научно-исследовательских и опытно-конструкторских работ, сертификационных испытаний и создание систем защиты информации; способы организации работ при проведении сертификации программно-аппаратных средств защиты; принципы построения средств криптографической 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; использовать профили защиты и задания по безопасности; применять инструментальные средства проведения сертификационных испытаний; составлять и оформлять аналитический отчет по проведенным сертификационным испытаниям; делать выводы по оценке защищенности на основании аналитического отчета. Владеть: навыками проведения теоретических исследований уровней защищенности компьютерных систем и сетей; проведения экспериментальных исследований уровней защищенности компьютерных систем и сетей; проведения сертификационных испытаний с использованием инструментальных средств; подготовки аналитического отчета по результатам проведенных

сертификационных испытаний; формулирования выводов по оценке защищенности.

ПК-4

Знать: принципы построения компьютерных систем и сетей; формальные модели безопасности компьютерных систем и сетей; принципы построения систем обнаружения компьютерных атак; методы обработки данных мониторинга безопасности компьютерных систем и сетей; порядок создания и структура отчета, создаваемого по результатам проверок; способы обнаружения и нейтрализации последствий вторжений в компьютерные системы; криптографические протоколы, применяемые в компьютерных сетях; 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: формализовывать задачу управления безопасностью компьютерных систем; применять инструментальные средства проведения мониторинга защищенности компьютерных систем; применять методы анализа защищенности компьютерных систем и сетей; структурировать аналитическую информацию для включения в отчет.

Владеть: навыками выполнения анализа защищенности компьютерных систем с использованием сканеров безопасности; выполнения анализа защищенности сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей; составления отчетов по результатам проверок.

ПК-9

Знать: методологические основы теории принятия решений, теории измерений, теории прогнозирования и планирования; способы измерения свойств объектов предметной области; структуру, принципы построения и функционирования ситуационных центров; основы построения и функционирования геоинформационных автоматизированных систем; методы оценки эффективности и качества в задачах прогнозирования, планирования, принятия решений при различной априорной неопределенности имеющейся информации; методы теории вероятностей, теории случайных процессов и математической статистики; роль и место информационно-аналитической деятельности в системах организационного управления; методологические основы информационно-аналитической деятельности; принципы организации информационно-аналитической деятельности; способы формирования описаний объектов и классов объектов предметной области; 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: разрабатывать формализованные модели, методы и алгоритмы решения типовых задач автоматизированной информационно-аналитической поддержки процессов принятия решений; применять методы и средства мониторинга и ситуационного анализа обстановки на базе ситуационных центров и геоинформационных

	автоматизированных систем; использовать современные модели и методы измерения, прогнозирования, планирования, принятия решений при решении задач поддержки процессов принятия решений; оценивать эффективность и качество в задачах прогнозирования, планирования, принятия решений при различной априорной неопределенности имеющейся информации. Владеть: навыками формализации задач автоматизированной информационно-аналитической поддержки процессов принятия решений в сфере компьютерной безопасности; решения задач прогнозирования, планирования, выработки решений при различной априорной неопределенности имеющейся информации; оценки эффективности и качества в задачах прогнозирования, планирования, принятия решений при различной априорной неопределенности имеющейся информации.
Трудоемкость, з е	8
Форма отчетности	Зачет с оценкой, 9 семестр; экзамен, 10 семестр
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