

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:
 b47f96eea65a2dc27b94ab71bb0b10000e7ad4d

Аннотация дисциплины

Наименование дисциплины	Методы оценки надежности компьютерных систем
Содержание	Введение в надежность компьютерных систем. Особенности компьютерных систем. Актуальность проблемы обеспечения надежности систем. Модели безопасности операционных систем. Технологии межсетевых экранов. Основы технологии виртуальных защищенных сетей VPN. Протоколы защиты на канальном и сеансовом уровнях. Защита сетевого уровня - протокол IPSec. Технологии обнаружения атак. Технологии защиты от вирусов
Реализуемые компетенции	ОПК-12. Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения. ПК-4. Способен проводить инструментальный анализ защищенности компьютерной системы и осуществлять поиск уязвимостей программного обеспечения. ПК-8. Способен устранять сбои и отказы сетевых устройств и операционных систем
Результаты освоения дисциплины (модуля)	ОПК-12 Знать: принципы построения современных операционных систем и особенности их применения; принципы разработки специального программного обеспечения, предназначенного для преодоления защиты современных операционных систем с использованием их недокументированных возможностей; основные принципы конфигурирования и администрирования операционных систем. Уметь: умеет разрабатывать системное и прикладное программное обеспечение для многозадачных, многопользовательских и многопроцессорных сред, а также для сред с интерфейсом, управляемым сообщениями; применять основные методы программирования в выбранной операционной сред. Владеть: навыками системного программирования. 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-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.	4
Формы отчетности	Зачет с оценкой, 7 семестр
Перечень основной и дополнительной литературы, необходимой для освоения дисциплины	
Основная литература	1. Артемов А. В. Информационная безопасность: курс лекций / А.В. Артемов; Межрегиональная Академия безопасности и выживания. Орел: МАБИВ, – 2014. – 257 с. 2. Аверченков В. И. Аудит информационной безопасности: учебное пособие для вузов / В.И. Аверченков. 2-е изд., стер. –

	М.: Флинта, 2011. 269 с. 3. Шаньгин В. Ф. Комплексная защита информации в корпоративных системах: учеб. пособие для вузов / В.Ф. Шаньгин. – Москва: Форум: ИНФРАМ, 2013. 4. Мельников В. П. Информационная безопасность и защита информации: учеб. пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова. – 6-е изд., стер. – Москва: Академия, 2012.
Дополнительная литература	1. Девянин П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие. Москва, 2012. 2. Девянин П. Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах. – М.: Радио и связь, 2006. 3. Дж. Фостер. Разработка средств безопасности и эксплойтов. Writing Security Tools and Exploits. – СПб.: Питер, 2007. 4. Девянин П. Н. Модели безопасности компьютерных систем. – М.: Академия, 2005 5. Филин С. А. Информационная безопасность. Учебное пособие. – М.: Альфа-Пресс, 2006. 6. Мельников В. В. Безопасность информации в автоматизированных системах. – М.: Финансы и статистика, 2003.