

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:
 b47f96eea63ad6c47b94ab7100b10000e7ad4d

Аннотация дисциплины

Наименование дисциплины	Защита в операционных системах
Содержание	Общие вопросы обеспечения информационной безопасности. Классификация угроз безопасности операционной системы. Типичные атаки на операционную систему. Сканирование файловой системы. Кража ключевой информации. Подходы к построению защищенных операционных систем. Административные меры защиты. Адекватная политика безопасности. Подсистемы защиты в современных операционных системах. Типовая структура подсистемы безопасности ОС и выполняемые ей функции. Структура защищенной ОС. Программно-технический уровень информационной безопасности. Основные понятия программно-технического уровня информационной безопасности. Требования к защите компьютерной информации. Модели безопасности основных операционных систем. Механизмы защиты операционных систем. Анализ защищенности современных операционных систем. Элементы безопасности системы. Защита в операционной системе Unix и Novell NetWare. Системы защиты программного обеспечения. Классификация систем защиты программного обеспечения. Достоинства и недостатки основных систем защиты. Показатели эффективности систем защиты. Протоколирование и аудит: Основные понятия; Активный аудит; Функциональные компоненты и архитектура. Защита в операционной системе Windows: Объекты и субъекты доступа. Разграничение доступа; Идентификация, аутентификация и авторизация пользователей. Аудит в Windows. Технологии и средства аудита. Система безопасности операционной системы Windows NT. Сервер аутентификации Kerberos. Защита в операционной системе Linux. Пользователи и их права ОС Linux: Учетные записи пользователей и работа с ними; Процедура регистрации и ее безопасность; Права доступа к файлам. Безопасное управление процессами ОС Linux. Защита в операционной системе IBM. Общий обзор средств безопасности OS/390.
Реализуемые компетенции	ОПК-13. Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности. ОПК-8. Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей. ОПК-11. Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации.
Результаты освоения дисциплины (модуля)	ОПК-13 Знать: средства и методы хранения и передачи аутентификационной информации; основные требования к подсистеме аудита и политике аудита; защитные механизмы и

	средства обеспечения безопасности операционных систем. Уметь: формулировать и настраивать политику безопасности основных операционных систем; формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на базе основных операционных систем. Владеть: навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств. ОПК-8 Знать: основные виды политик управления доступом и информационными потоками в компьютерных системах; основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков; средства и методы хранения и передачи аутентификационной информации; основные требования к подсистеме аудита и политике аудита; защитные механизмы и средства обеспечения безопасности операционных систем; механизмы реализации атак в сетях TCP/IP; основные протоколы идентификации и аутентификации абонентов сети; защитные механизмы и средства обеспечения сетевой безопасности; средства и методы предотвращения и обнаружения вторжений. Уметь: разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками; формулировать и настраивать политику безопасности основных операционных систем; формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на базе основных операционных систем; умеет формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; Владеть: навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств; навыками настройки межсетевых экранов. ОПК-11 Знать: средства и методы хранения и передачи аутентификационной информации; основные требования к подсистеме аудита и политике аудита; защитные механизмы и средства обеспечения безопасности операционных систем. Уметь: формулировать и настраивать политику безопасности основных операционных систем; формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на базе основных операционных систем. Владеть: средства и методы хранения и передачи аутентификационной информации; основные требования к подсистеме аудита и политике аудита; защитные механизмы и средства обеспечения безопасности операционных систем; навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных
--	--

	систем распространенных семейств.
Трудоёмкость, з.е.	4
Формы отчётности (в т.ч. по семестрам)	Зачет с оценкой, 5 семестр
Перечень основной и дополнительной литературы, необходимой для освоения дисциплины	
Основная литература	1. Филиппов, М.В. Операционные системы Электронный ресурс: –учебно-методическое пособие / Д.В. Завьялов / М.В. Филиппов. Операционные системы, 2018-12-09. – Волгоград: Волгоградский институт бизнеса, 2014. – 163 с. – Книга находится в базовой версии ЭБС IPRbooks
Дополнительная литература	1. Назаров, С.В. Современные операционные системы Электронный ресурс: учебное пособие / А.И. Широков / С.В. Назаров. – Современные операционные системы, 2019-12-01. – Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. – 351 с. – Книга находится в базовой версии ЭБС IPRbooks. – ISBN 978-5-9963-0416-5