

Документ подписан простой электронной подписью
Информация о владельце:

ФИО: Петренко Вячеслав Иванович
Должность: и.о. директора Института цифрового развития
Дата подписания: 08.04.2024 09:29:18

Уникальный идентификатор:
b47f96eea65a16e179f94dbf7fb0b10000e7ad4d

Аннотация дисциплины

Наименование
дисциплины

Защищенные информационные системы

Краткое содержание

Механизмы защиты операционной системы
Угрозы безопасности операционной системы. Понятие защищенной операционной системы. Подходы к организации защиты. Структура системы обеспечения информационной безопасности. Принципы организации технического, программного и информационного обеспечения. Этапы построения защиты.
Субъекты, объекты, методы и права доступа, привилегии субъекта доступа. Дискреционное управление доступом. Изолированная программная среда. Мандатное управление доступом. Контроль информационных потоков.
Идентификация, аутентификация и авторизация. Аутентификация на основе паролей. Парольная аутентификация в операционных системах семейства Windows и UNIX. Аутентификация на основе внешних носителей ключа. Биометрическая аутентификация: общая схема, преимущества, проблемы.
Управление доступом в операционных системах семейства Windows и UNIX.
Аудит. Требования к подсистеме аудита. Необходимость аудита в защищенной системе. Реализация аудита в операционных системах семейства Windows и UNIX.
Интеграция защищенных операционных систем
Домены Windows. Преимущества доменной архитектуры локальной сети. Понятие домена, контроллер домена. Сквозная аутентификация. Централизованное управление политикой безопасности в домене.
Идентификация компьютеров в сети. Двусторонние транзитивные отношения доверия. Групповая политика. Делегирование полномочий. Защита в компьютерных сетях. Типовые угрозы сетевой безопасности.
Сетевые атаки. Стадии проведения сетевой атаки. Классификации сетевых угроз, уязвимостей и атак. Примеры типичных сетевых атак.
Механизмы реализации атак в сетях TCP/IP. Удаленное определение версии ОС. Методы сканирования портов. Методы обнаружения пакетных sniffеров.
Методы перехвата сетевых соединений в сетях TCP/IP.
Десинхронизация TCP-соединений. Атаки, направленные на маршрутизаторы. Несанкционированный обмен данными.
Технические меры защиты от сетевых атак.
Методы и средства обеспечения информационной безопасности в вычислительных сетях
Виртуальные частные сети (VPN). Организация туннелирования на различных уровнях модели ISO/OSI. Достоинства и недостатки применения VPN. Протокол IPSEC. Использование протокола PPTP для организации виртуальных частных сетей.
Криптографические протоколы аутентификации. Разработка защищенных сетевых приложений.
Средства защиты локальных сетей при подключении к Интернет.
Межсетевые экраны (МЭ). Основные возможности и схемы

	развертывания МЭ. Построение правил фильтрации. Методы сетевой трансляции адресов (NAT). Методы обхода межсетевых экранов. Системы обнаружения вторжений (СОВ). Средства обнаружения уязвимостей сетевых служб. Способы противодействия вторжениям. Системы виртуальных ловушек (Honey Pot и Padded Cell). Защита в системах управления базами данных Теоретические основы безопасности в СУБД Понятие безопасности БД. Угрозы безопасности БД. Целостность БД. Аудит. Средства обеспечения защиты информации в СУБД и многоуровневая защита. Политика безопасности в СУБД. Модели безопасности в СУБД. Механизмы обеспечения конфиденциальности, целостности и высокой готовности СУБД. Угрозы конфиденциальности СУБД. Основные методы нарушения конфиденциальности. Способы противодействия. Методы аутентификации пользователей СУБД. Их преимущества и недостатки. Средства управления доступом. Использование ролей и привилегий пользователей. Аудит и подотчетность. Криптографические методы защиты баз данных. Угрозы целостности СУБД. Основные виды и причины возникновения угроз целостности. Способы противодействия. Понятие транзакции. Блокировки. Ссылочная целостность. Правила (триггеры). Средства, поддерживающие высокую готовность. Аппаратная и программная поддержки. Сохранение и восстановление БД. Мониторинг серверов СУБД. Аппаратная избыточность и избыточность данных.
Результаты освоения дисциплины	- формулирует основы отечественных и зарубежных стандартов в области обеспечения информационной безопасности; - выделяет направления развития технологий проектирования информационных, автоматизированных и автоматических систем; - применяет методы проектирования и построения систем информационной безопасности, включая методы тестирования эффективности и оценки надёжности; - Полностью оценивает роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства - использует современные программные и программно-аппаратные (в том числе криптографические) средства защиты информации в профессиональной деятельности; - применяет методы решения задач для защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью; - разрабатывает тестовые планы и сценарии тестирования разработанного продукта; - проектирует подсистемы безопасности информационных систем с учетом действующих нормативных и методических документов - разрабатывает модели угроз и нарушителей информационной безопасности информационных систем; - реализует выполнение типовых задач разработки и исследования систем защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью;

	использует средства автоматизированного и ручного функционального тестирования;
Трудоемкость, з.е.	8 з.е.
Форма отчетности	Экзамен, курсовая работа
Перечень основной и дополнительной литературы, необходимой для освоения дисциплины	
Основная литература	1. Мошак, Н. Н. Защищенные информационные системы : учебное пособие / Н. Н. Мошак, Л. К. Птицына. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2020. — 216 с 2. Технологии обеспечения безопасности информационных систем : учебное пособие : [16+] / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов [и др.]. – Москва ; Берлин : Директ-Медиа, 2021. – 210 с.
Дополнительная литература	1. Защита информации в операционных системах : (спец. 090103 Организация и технология защиты информации, 090102 – Компьютерная безопасность) : учеб. пособие / авт. сост.: И. В. Зайцева / М. В. Романкова / Федеральное агентство по образованию, Ставроп. гос. ун-т. - Ставрополь : Изд-во СГУ, 2008. - 318 3-402 с. - Библиогр.: с. 311-312. 2. Хорев П.Б. Методы и средства защиты информации в компьютерных системах. – М.: Издательский центр «Академия», 2008. – 256 с