АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ
«Информационная безопасность баз данных»

по основной профессиональной образовательной программе по направлению подготовки 09.03.01 «Информатика и вычислительная техника» (уровень бакалавриата)

Направленность (профиль): Программно-техническое обеспечение автоматизированных систем
Общий объем дисциплины – 3 з.е. (108 часов)
Форма промежуточной аттестации – Зачет.
В результате освоения дисциплины у обучающихся должны быть сформированы компетенции с соответствующими индикаторами их достижения:

- ПК-8.1: Выбирает автоматизированные средства контроля состояния баз данных;
- ПК-8.2: Выявляет угрозы безопасности на уровне баз данных;

Содержание дисциплины:
Дисциплина «Информационная безопасность баз данных» включает в себя следующие разделы:
Форма обучения очная. Семестр 8.
1. Модуль 1. Выявление угроз безопасности баз данных, средства обеспечения конфиденциальности. Тема 1. Критерии оценки надежности компьютерных систем. Понятие политики безопасности. Совместное применение политик безопасности в рамках единой модели. Задачи обеспечения безопасности баз данных. Классификация угроз баз данных. Выявление угроз безопасности баз данных. Выявление угроз безопасности на основе баз известных уязвимостей СУБД. Основные компоненты системы защиты баз данных
Тема 2. Средства обеспечения конфиденциальности баз данных. Идентификация и проверка подлинности пользователей. Средства идентификации и аутентификации объектов баз данных. Учетная запись. Режимы аутентификации. Управление ключами безопасности.
2. Модуль 2. Модели управления доступом в базах данных. Тема 3. Дискреционная модель управления доступом. Основные категории пользователей. Ролевая модель разграничения доступа. Пользовательские роли и роли приложений. Разграничение доступа на уровне таблиц, строк и полей в реляционных СУБД. Команды SQL для установки и управления правилами разграничения доступа.
Тема 4. Мандатное управление доступом. Метки конфиденциальности. Уровни конфиденциальности объектов и уровни доверия субъектов доступа. Принудительный контроль доступа. Правила мандатного доступа. Особенности реализации мандатного доступа в реляционных СУБД.
3. Модуль 3. Обеспечение доступности данных. Тема 5. Средства обеспечения доступности баз данных. Резервирование и архивирование баз данных. Полное резервирование. Дифференциальное резервирование. Инкрементальное резервирование. Клонирование. Резервирование в режиме реального времени. Резервное копирование в виде образа. Схемы ротации резервных копий. Средства создания и восстановления баз данных. Определение и виды кластерных систем. Архитектуры хранения данных в кластерных системах. Зеркалирование баз данных.
4. Модуль 4. Автоматизация контроля состояния баз данных, безопасность распределенных СУБД. Тема 6. Методы контроля состояния баз данных. Выбор средств автоматизированного контроля состояния баз данных. Автоматизированный контроль состояния баз данных с использованием мониторинга активности (DAM). Привилегированный мониторинг пользователей. Мониторинг активности приложений. Защита от кибер-атак. Типы архитектуры DAM. DAM на основе перехвата. DAM на основе памяти. DAM на основе журнала событий. Аудит событий. Средства и процессы подсистемы аудита. Ведение журнала аудита. Спецификация аудита. Отчеты о зависимостях.
Тема 7. Тиражирование и синхронизация в распределенных СУБД. Угрозы безопасности распределенных СУБД. Распределенные транзакции. Методы распределения данных. Общие сведения о репликации. Модели репликации. Управление репликацией..

Разработал:
старший преподаватель

кафедры ИВТиИБ П.А. Теплюк

Проверил:
Декан ФИТ А.С. Авдеев