АННОТАЦИЯ
рабочей программы дисциплины «Безопасность баз данных» по направлению подготовки 10.03.01 Информационная безопасность

1. Цели освоения дисциплины.

Целью освоения учебной дисциплины «Безопасность баз данных» является изучение основных принципов построения безопасных систем баз данных, защиты баз данных и их практической реализации.

2. Требования к уровню освоения содержания дисциплины.

Процесс изучения дисциплины «Безопасность баз данных» направлен на формирование следующих профессиональных компетенций:

- способностью принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия (ПК-9);
- способностью администрировать подсистемы информационной безопасности объекта (ПК-10);
- способностью выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации (ПК-11);
- способностью участвовать в разработке подсистемы управления информационной безопасностью (ПК-12);
- способностью применять программные средства системного, прикладного и специального назначения (ПК-15);
- способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью (ПК-25);
- способностью формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью (ПК-26);
- способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-27).

3. Требования к результатам освоения дисциплины.

В результате изучения дисциплины обучающиеся должны:

знать:

- архитектуру систем управления базами данных;
- структуру, свойству информационной безопасности баз данных;
- объекты и субъекты моделей информационной безопасности баз данных;
- принципы построения защищенных систем баз данных;
- методы обеспечения безопасности баз данных;

уметь:

- применять полученные знания в практической работе;
- создавать защищенную базу данных и проводить аудит созданной.

владеть:

- навыками работы с современными СУБД;
- навыками разработки защищенной базы данных и проводить аудит созданной;
- навыками разработки стратегии применения средств обеспечения

информационной безопасности.

4. Содержание дисциплины.

ПОСТАНОВКА ЗАДАЧИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАЗ ДАННЫХ. Этапы научного формирования проблемы обеспечения информационной безопасности баз данных. Критерии качества баз данных. Сущность понятия безопасности баз данных. Основные подходы к методам построения защищенных информационных систем. Архитектура систем управления базами данных. Структура, свойства информационной безопасности баз данных.

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАЗ ДАННЫХ. Источники угроз информации баз данных. Классификация угроз информационной безопасности баз данных. Угрозы, специфичные для систем управления базами данных. Объекты и субъекты моделей информационной безопасности баз данных.

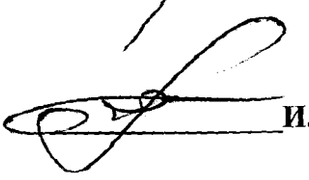
АТАКИ, СПЕЦИФИЧЕСКИЕ ДЛЯ БАЗ ДАННЫХ. Подбор и манипуляция с паролями как метод реализации несанкционированных прав. Нецелевое расходование вычислительных ресурсов сервера . Использование триггеров для выполнения незапланированных функций. Использование SQL-инъекции для нештатного использования процедур и функций.

ПОЛИТИКА БЕЗОПАСНОСТИ. Сущность политики безопасности. Цель формализации политики безопасности. Принципы построения защищенных систем баз данных. Стратегия применения средств обеспечения информационной безопасности.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ БАЗ ДАННЫХ. Методы обеспечения безопасности. Избирательное управление доступом. Обязательное управление доступом. Шифрование данных. Контрольный след выполняемых операций. Поддержка мер обеспечения безопасности в языке SQL. Директивы GRANT и REVOKE. Представления и безопасность.

Разработчик: Травкин Е.И.

Зав. информационной, техносферной безопасности и правовой защиты информации  **О.В. Воробьева**

Председатель Межкафедрального координационного учебно-методического совета  **И.В. Анциферова**