

**МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»**

Кафедра «Железнодорожная автоматика, телемеханика и связь»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

«Основы построения защищенных баз данных»

Направление подготовки:	<u>09.04.03 – Прикладная информатика</u>
Магистерская программа:	<u>Прикладная информатика в обеспечении безопасности бизнеса</u>
Квалификация выпускника:	<u>Магистр</u>
Форма обучения:	<u>заочная</u>
Год начала подготовки	<u>2019</u>

1. Цели освоения учебной дисциплины

Целью освоения учебной дисциплины «Основы построения защищенных баз данных» является формирование у обучающихся компетенций в соответствии с требованиями самостоятельно утвержденного образовательного стандарта высшего образования (СУОС)

по направлению 09.04.03 «Прикладная информатика» и приобретение ими:

- знаний об основных концепциях безопасности баз данных;
- умений использовать уровни политики безопасности баз данных;
- навыков аудита и мониторинга баз данных.

2. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Основы построения защищенных баз данных" относится к блоку 1 "Дисциплины (модули)" и входит в его базовую часть.

3. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих компетенций:

ПКС-51	Способен обеспечить кибербезопасность в бизнес-процессах при проектировании и эксплуатации информационных систем, управлении проектами в области информационных технологий
--------	--

4. Общая трудоемкость дисциплины составляет

4 зачетные единицы (144 ак. ч.).

5. Образовательные технологии

Образовательные технологии, используемые для реализации компетентностного подхода и с целью формирования и развития профессиональных навыков студентов по усмотрению преподавателя в учебном процессе могут быть использованы в различных сочетаниях активные и интерактивные формы проведения занятий, включая: Лекционные занятия. Информатизация образования обеспечивается с помощью средств новых информационных технологий - ЭВМ с соответствующим периферийным оборудованием; средства и устройства манипулирования аудиовизуальной информацией; системы машинной графики, программные комплексы (операционные системы, пакеты прикладных программ). Практические занятия. Информатизация образования обеспечивается с помощью средств новых информационных технологий - ЭВМ с соответствующим периферийным оборудованием; системы машинной графики, программные комплексы (операционные системы, пакеты прикладных программ). Самостоятельная работа. Дистанционное обучение - интернет-технология, которая обеспечивает студентов учебно-методическим материалом, размещенным на сайте академии, и предполагает интерактивное взаимодействие между преподавателем и студентами. Контроль самостоятельной работы. Использование тестовых заданий, что предполагает интерактивное взаимодействие между преподавателем и студентами. При изучении дисциплины используются технологии электронного обучения (информационные, интернет ресурсы, вычислительная техника) и, при необходимости, дистанционные образовательные технологии, реализуемые в основном с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии обучающегося и педагогических работников..

6. Содержание дисциплины (модуля), структурированное по темам (разделам)

РАЗДЕЛ 1

Раздел 1. Основные концепции безопасности баз данных.

Современные серверы баз данных. Усиление контроля доступом к базам данных через Web. Обновление программного обеспечения сервера баз данных.

РАЗДЕЛ 2

Раздел 2. Уровни политики безопасности сервера баз данных.

Безопасность на уровне сервера баз данных.

Безопасность на сетевом уровне .

Безопасность на уровне операционной системы.

РАЗДЕЛ 3

Раздел 3. Безопасность на уровне базы данных

Безопасность администрирования базы данных.

Роли и полномочия базы данных.

Безопасность на уровне объектов

РАЗДЕЛ 4

Раздел 4. Использование политики безопасности приложения.

Ограничение политики безопасности на уровне приложения.

Поддержка Web-приложений

РАЗДЕЛ 5

Раздел 5. Резервное копирование баз данных и восстановление данных

Определение ограничений для резервного копирования.

Определение требований к восстановлению данных.

РАЗДЕЛ 6

Раздел 6. Аудит и мониторинг баз данных.

Просмотр протоколов аудита.

Мониторинг сервера базы данных.

РАЗДЕЛ 7

Допуск к зачету

РАЗДЕЛ 1

Зачет с оценкой

РАЗДЕЛ 7

Допуск к зачету

защита КП

РАЗДЕЛ 1

Зачет с оценкой