

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:
 b47f96eea65a16e19394b7f00b10000e7ad4d

Аннотация дисциплины

Наименование дисциплины	Основы построения защищенных баз данных
Содержание	Теоретические основы безопасности в базах данных (БД). Безопасность баз данных, угрозы, защита. Понятие безопасности БД. Классификация угроз. Угрозы безопасности БД: общие и специфичные. Требования безопасности БД. Критерии защищенности БД. Критерии оценки надежных компьютерных систем (TCSEC). Понятие политики безопасности. Совместное применение различных политик безопасности в рамках единой модели. Интерпретация TCSEC для надежных СУБД (TDI). Оценка надежности СУБД как компоненты вычислительной системы. Модели безопасности в СУБД. Дискреционная (избирательная) модель. Мандатная (полномочная) модели безопасности. Классификация моделей. Аспекты исследования моделей безопасности. Особенности применения моделей безопасности в СУБД. Средства и методы обеспечения безопасности баз данных. Целостность БД и способы ее обеспечения. Основные виды и причины возникновения угроз целостности. Способы противодействия возникновению угроз целостности. Метаданные и словарь данных. Назначение словаря данных. Доступ к словарю данных. Состав словаря. Представление словаря. Транзакции и блокировки. Транзакции как средство изолированности пользователей. Сериализация транзакций. Назначение сериализации транзакций. Методы сериализации транзакций. Режимы блокировок. Правила согласования блокировок. Двухфазный протокол синхронизационных блокировок. Тупиковые ситуации, распознавание тупиковых ситуаций и разрушение. Ссылочная целостность. Декларативная и процедурная ссылочные целостности. Внешний ключ. Способы поддержания ссылочной целостности. Понятие ссылочной целостности. Классификация угроз конфиденциальности СУБД. Причины, виды, основные методы нарушения конфиденциальности. Типы утечки конфиденциальной информации из СУБД, частичное разглашение. Получение несанкционированного доступа к конфиденциальной информации путем логических выводов. Методы противодействия. Особенности применения криптографических методов. Целостность кода приложения SQL-инъекции. Динамическое выполнение кода SQL и PL/SQL. Категории атак SQL-инъекцией. Методы SQL-инъекций. Противодействие атакам типа SQL-инъекции. Средства идентификации и аутентификации. Общие сведения. Совместное применение средств идентификации и привилегий пользователей. Соотношение прав доступа, определяемых ОС и СУБД. Использование представлений для обеспечения конфиденциальности информации в СУБД. Средства реализации мандатной политики безопасности в СУБД.
Реализуемые компетенции	ОПК-14. Способен проектировать базы данных, администрировать системы управления базами данных в соответствии с требованиями по защите информации.

	ПК-2. Способен проводить анализ безопасности компьютерных систем.
Результаты освоения дисциплины модуля	ОПК-14 Знать: общие и специфические угрозы безопасности баз данных; основные критерии защищенности баз данных и методы оценивания механизмов защиты; механизмы обеспечения конфиденциальности, целостности и высокой доступности баз данных; особенности применения криптографической защиты в системах управления базами данных; этапы проектирования системы защиты в системах управления базами данных. Уметь: пользоваться средствами защиты, предоставляемыми системами управления базами данных; создавать дополнительные средства защиты баз данных; умеет проводить анализ и оценивание механизмов защиты баз данных. Владеть: методикой и навыками использования средств защиты, предоставляемых системами управления базами данных. ПК-2 Знать: криптографические методы защиты информации; принципы построения систем управления базами данных. Уметь: прогнозировать возможные пути развития действий нарушителя информационной безопасности. Владеть: навыками определения уровня защищенности и доверия в компьютерных системах.
Трудоёмкость, з.е.	4
Формы отчётности в т.ч. по семестрам	Экзамен, 10 семестр
Перечень основной и дополнительной литературы, необходимой для освоения дисциплины	
Основная литература	Тони, Хаулет. Защитные средства с открытыми исходными текстами. Практическое руководство по защитным приложениям Электронный ресурс: учебное пособие / Хаулет Тони; ред. В. Галатенко. – Защитные средства с открытыми исходными текстами. Практическое руководство по защитным приложениям, 2020-07-28. – Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. - 608 с. – Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-4487-0065-1
Дополнительная литература	1. Введение в СУБД MySQL Электронный ресурс: учебное пособие. – Введение в СУБД MySQL, 2021-01-23. – Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. – 228 с. – Книга находится в базовой версии ЭБС IPRbooks. 2. Кисленко, Н.П. Интернет-программирование на PHP Электронный ресурс: учебное пособие / Н.П. Кисленко. – Новосибирск: Новосибирский государственный архитектурно-строительный университет (Сибстрин), ЭБС АСВ, 2015. – 177 с. – Книга находится в базовой версии ЭБС IPRbooks. – ISBN 978-5-7795-0745-5 3. Туманов, В. Е. Проектирование хранилищ данных для систем деловой осведомленности (Business Intelligence Systems) Электронный ресурс / В. Е. Туманов. – Проектирование хранилищ данных для систем деловой осведомленности (Business Intelligence

	Systems),2020-03-31. – Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. – 937 с. – Книга находится в премиум-версии ЭБС IPR BOOKS. – ISBN 978-5-9963-0353-3
--	---