|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Федеральное государственное автономное образовательное   учреждение высшего образования   «Московский физико-технический институт   (государственный университет)»** | | | | | | | | | | |
|
|
|
|  | | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
|  |  |  | |  | **«УТВЕРЖДАЮ»** | | | | |  |
|  |  |  |  | **Директор физтех-школы радиотехники и компьютерных технологий** | | | | |  | |
|  |  |  |  |  | |
|  |  |  |  | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.В. Дворкович** | | | |  | |  |
|  |  |  |  |  |  |  | | |  | |
| **Рабочая программа дисциплины (модуля)** | | | | | | | | | | |
| **по дисциплине:** | | Основы построения защищенных баз данных | | | | | | | | |
| **по направлению:** | | Компьютерная безопасность (специалитет) | | | | | | | | |
| **профиль подготовки:** | | Безопасность распределённых компьютерных систем | | | | | | | | |
|  |  | факультет радиотехники и кибернетики | | | | | | | | |
|  |  | кафедра защиты информации | | | | | | | | |
| **курс:** | | 5 | | | | | | | | |
| **квалификация:** | | специалист | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
| Семестр, формы промежуточной аттестации: 10(Весенний) - Экзамен | | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
| Аудиторных часов: 45 всего, в том числе: | | | | | |  | | |  | |
|  | лекции: 30 час. | | | | |  | | |  | |
|  | практические и семинарские занятия: 0 час. | | | | |  | | |  | |
|  | лабораторные занятия: 15 час. | | | | |  | | |  | |
|  |  |  |  |  |  |  | | |  | |
| Самостоятельная работа: 69 час. | | | | | |  | | |  | |
|  |  |  |  |  |  |  | | |  | |
| Подготовка к экзамену: 30 час. | | | | | |  | | |  | |
|  |  |  |  |  |  |  | | |  | |
| Всего часов: 144, всего зач. ед.: 4 | | | | | |  | | |  | |
|  |  |  |  |  |  |  | | |  | |
| **Программу составили:** | | | | | |  | | |  | |
|  |  |  |  |  |  |  | | |  | |
| А.А. Алтухов, ассистент | | | | | | | | | | |
| В.А. Конявский, д-р техн. наук | | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
| **Программа обсуждена на заседании кафедры** | | | | | |  | | |  | |
|  |  |  |  |  |  |  | | |  | |
| 13 мая 2017 г. | | | | | |  | | |  | |
|  |  |  |  |  |  |  | | |  | |
| СОГЛАСОВАНО: | | | | | |  | | |  | |
|  |  |  |  |  |  |  | | |  | |
|  | Заведующий кафедрой | | | | В.А. Конявский | | | | |  |
|  |  |  |  |  |  |  | | |  | |
|  | Начальник учебного управления | | | | И.Р. Гарайшина | | | | |  |
|  |  |  |  |  |  |  | | |  | |
|  | Декан факультета | | | | С.Н. Гаричев | | | | |  |
|  |  |  |  |  |  |  | | |  | |
|  |  |  |  |  |  |  | | |  | |
| **1. Цели и задачи** | | | | | |  | | |  | |
|  |  |  |  |  |  |  | | |  | |
| **Цель дисциплины** | |  |  |  |  |  | | |  | |
| Цель освоения дисциплины – формирование базовых знаний по использованию и проектированию защищенных баз данных. | | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
| **Задачи дисциплины** | | | | | |  | | |  | |
| Задачи освоения дисциплины студентами – приобретение основных теоретических сведений, практических навыков по разделам: основные сведения о хранении данных, реляционная модель данных, система управления базами данных (СУБД) Microsoft Access, сохранение точности информации и защита баз данных, языки баз данных, реляционные СУБД, проектирование реляционных баз данных на основе принципов нормализации, концептуальное и даталогическое проектирование баз данных, СУБД Microsoft SQL Server. | | | | | | | | | | |
| При изучении дисциплины укрепляются теоретические и практические навыки работы с современными СУБД и приобретается опыт проектирования реляционных баз данных. Полученные знания лежат в основе профессионального образования и найдут самое широкое применение в будущей профессиональной деятельности учащихся. | | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
| **2. Место дисциплины (модуля) в структуре образовательной программы** | | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
|  |  |  |  |  |  |  | | |  | |
| Настоящая учебная дисциплина является базовой дисциплиной в учебной программе подготовки специалистов направления «Компьютерная безопасность».  Курс основывается на дисциплинах «Базы данных», «Основы информационной безопасности». | | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
| Дисциплина «Основы построения защищенных баз данных» базируется на дисциплинах: | | | | | | | | | | |
| Базы данных; | | | | | | | | | | |
| Основы информационной безопасности. | | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
| Дисциплина «Основы построения защищенных баз данных» предшествует изучению дисциплин: | | | | | | | | | | |
| Модели безопасности компьютерных систем; | | | | | | | | | | |
| Теория управления информационной безопасностью распределенных компьютерных систем; | | | | | | | | | | |
| Научно-исследовательская работа. | | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
| **3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы** | | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
| Освоение дисциплины направлено на формирование следующих общекультурных, общепрофессиональных и профессиональных компетенций: | | | | | | | | | | |
| способность к самоорганизации и самообразованию (ОК-8); | | | | | | | | | | |
| способность производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение (ПК-17); | | | | | | | | | | |
| способность производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации (ПК-18); | | | | | | | | | | |
| способность использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач (ОПК-8); | | | | | | | | | | |
| способность понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации (ОПК-3). | | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
| **В результате освоения дисциплины обучающиеся должны** | | | | | |  | | |  | |
|  |  |  |  |  |  |  | | |  | |
| **знать:** | |  |  |  |  |  | | |  | |
| • особенности математических моделей и их влияние на разработку системы БД;  • изобразительные средства, используемые в моделировании БД;  • языки описания и манипулирования данными разных классов (QBE, SQL, элементы 4GL);  • технологии организации БД. | | | | | | | | | | |
| **уметь:** | | | | | |  | | |  | |
| • определить предметную область;  • спроектировать реляционную базу данных (определить состав каждой таблицы, типы полей, ключ для каждой таблицы);  • работать с современными программными средствами (Case);  • определить ограничения целостности, получать результатные данные в виде различном виде (ответов на запросы, экранных форм, отчетов). | | | | | | | | | | |
| **владеть:** | | | | | |  | | |  | |
| • навыками работы в среде современных СУБД;  • способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства;  • способностью оценивать свои достоинства и недостатки, определять пути и выбирать средства развития достоинств и устранения недостатков;  • способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечения требуемого уровня эффективности применения автоматизированных систем. | | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
| **4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий** | | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
| 4.1. Разделы дисциплины (модуля) и трудоемкости по видам учебных занятий | | | | | |  | | |  | |
|  |  |  |  |  |  |  | | |  | |
|  |  |  |  |  |  |  | | |  | |
| № | Тема (раздел) дисциплины | | Виды учебных занятий, включая самостоятельную работу | | | | | | | |
| Лекции | Практичес- кие и семинарские занятия | Лаборат. работы | Задания, курсовые работы | | | Самост. работа | |
|
| 1 | Концепция безопасности БД. | | 3 |  | 1 |  | | | 9 | |
| 2 | Теоретические основы безопасности в СУБД | | 3 |  | 2 |  | | | 7 | |
| 3 | Механизмы обеспечения целостности СУБД. | | 4 |  | 2 |  | | | 9 | |
| 4 | Механизмы обеспечения конфиденциальности в СУБД | | 4 |  | 1 |  | | | 7 | |
| 5 | Механизмы, поддерживающие высокую готовность. | | 3 |  | 1 |  | | | 9 | |
| 6 | Защита данных в распределенных системах | | 3 |  | 2 |  | | | 7 | |
| 7 | Безопасность в статистических БД. | | 3 |  | 2 |  | | | 7 | |
| 8 | Распознавание вторжений в БД | | 3 |  | 2 |  | | | 7 | |
| 9 | Проектирование безопасности БД. | | 4 |  | 2 |  | | | 7 | |
| Итого часов | | | 30 |  | 15 |  | | | 69 | |
| Подготовка к экзамену | | | 30 час. | | | | | | | |
| Общая трудоёмкость | | | 144 час., 4 зач.ед. | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
| 4.2. | Содержание дисциплины (модуля), структурированное по темам (разделам) | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
| Семестр: 10 (Весенний) | | | | | |  | | |  | |
|  |  |  |  |  |  |  | | |  | |
|  | 1. Концепция безопасности БД. | | | | | | | | | |
|  | | | | | |  | | |  | |
|  | Понятие безопасности БД. Угрозы безопасности БД: общие и специфичные. Требования безопасности БД. Защита от несанкционированного доступа. Защита от вывода. Целостность БД. Аудит. Многоуровневая защита. Типы контроля безопасности: потоковый, контроль вы-вода, контроль доступа. | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
|  | 2. Теоретические основы безопасности в СУБД | | | | | | | | | |
|  | | | | | |  | | |  | |
|  | 2.1. 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. Монитор ссылок. Применение TCSEC к СУБД непосредственно. Элементы СУБД, к которым применяются TDI: метки, аудит, архитектура системы, спецификация, верификация, проектная документация. Критерии безопасности ГТК. | | | | | | | | | |
|  |  | | | | | | | | | |
|  | 2.2. Модели безопасности в СУБД | | | | | | | | | |
|  | Дискреционная (избирательная) и мандатная (полномочная) модели безопасности. Класси-фикация моделей. Аспекты исследования моделей безопасности. Особенности применения мо-делей безопасности в СУБД. Дискреционные модели: HRU, Take-Grant, Action-Entity, Wood. Мандатные модели: Bell-LaPadula, Biba, Dion, Sea View, Jajodia&Sandhu, Smith&Winslett, реше-точная. БД с многоуровневой секретностью (MLS). Многозначность. | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
|  | 3. Механизмы обеспечения целостности СУБД. | | | | | | | | | |
|  | | | | | |  | | |  | |
|  | 3.1. Угрозы целостности СУБД. | | | | | | | | | |
|  | Основные виды и причины возникновения угроз целостности. Способы противодействия. | | | | | | | | | |
|  | 3.2. Метаданные и словарь данных. | | | | | | | | | |
|  | Назначение словаря данных. Доступ к словарю данных. Состав словаря. Представления словаря. | | | | | | | | | |
|  | 3.3. Понятие транзакции. | | | | | | | | | |
|  | Фиксация транзакции. Прокрутки вперед и назад. Контрольная точка. Откат. Транзакции как средство изолированности пользователей. Сериализация транзакций. Методы сериализации транзакций. | | | | | | | | | |
|  | 3.4. Блокировки. | | | | | | | | | |
|  | Режимы блокировок. Правила согласования блокировок. Двухфазный протокол синхрони-зационных блокировок. Тупиковые ситуации, их распознавание и разрушение. | | | | | | | | | |
|  | 3.5. Ссылочная целостность. | | | | | | | | | |
|  | Декларативная и процедурная ссылочные целостности. Внешний ключ. Способы поддер-жания ссылочной целостности. | | | | | | | | | |
|  | 3.6. Правила(триггеры). | | | | | | | | | |
|  | Цели использования правил. Способы задания, моменты выполнения. | | | | | | | | | |
|  | 3.7. События. | | | | | | | | | |
|  | Назначение механизма событий. Сигнализаторы событий. Типы уведомлений о происхож-дении события. Компоненты механизма событий. | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
|  | 4. Механизмы обеспечения конфиденциальности в СУБД | | | | | | | | | |
|  | | | | | |  | | |  | |
|  | 4.1 Классификация угроз конфиденциальности СУБД | | | | | | | | | |
|  | Причины, виды, основные методы нарушения конфиденциальности. Типы утечки конфи-денциальной информации из СУБД, частичное разглашение. Соотношение защищенности и доступности данных. Получение несанкционированного доступа к конфиденциальной инфор-мации путем логических выводов. Методы противодействия. Особенности применения криптографических методов. | | | | | | | | | |
|  | 4.2 Средства идентификации и аутентификации | | | | | | | | | |
|  | Общие сведения. Совместное применение средств идентификации и аутентификации, встроенных в СУБД и в ОС. | | | | | | | | | |
|  | 4.3 Средства управления доступом | | | | | | | | | |
|  | Основные понятия: субъекты и объекты, группы пользователей, привилегии, роли и пред-ставления. Виды привилегий: привилегии безопасности и доступа. Использование ролей и привилегий пользователей. Соотношение прав доступа, определяемых ОС и СУБД. Метки безопасности. Использование представлений для обеспечения конфиденциальности информации в СУБД. | | | | | | | | | |
|  | 4.4 Обеспечение конфиденциальности путем тиражирования БД | | | | | | | | | |
|  | Формальная модель для обеспечения конфиденциальности БД с помощью тиражирования. Архитектура и политика безопасности в модели SINTRA. | | | | | | | | | |
|  | 4.5 Аудит и подотчетность | | | | | | | | | |
|  | Подотчетность действий пользователя и аудит связанных с безопасностью событий. Реги-страция действий пользователя. Управление набором регистрируемых событий. Анализ регистрационной информации. | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
|  | 5. Механизмы, поддерживающие высокую готовность. | | | | | | | | | |
|  | | | | | |  | | |  | |
|  | 5.1. Средства, поддерживающие высокую готовность | | | | | | | | | |
|  | Аппаратная и программная поддержки. Кластерная организация серверов баз данных. Па-раметры настройки СУБД. Сохранение и восстановление БД | | | | | | | | | |
|  | 5.2. Оперативное администрирование | | | | | | | | | |
|  | Задачи, средства и режимы администрирования. Мониторинг серверов СУБД. | | | | | | | | | |
|  | 5.3. Функциональная насыщенность СУБД | | | | | | | | | |
|  | Формы избыточности. Аппаратная избыточность. Избыточность данных. Программное зер-калирование. Тиражирование данных. | | | | | | | | | |
|  | 5.4. Системы, обладающие свойством высокой готовности | | | | | | | | | |
|  | Описание, назначение, примеры. | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
|  | 6. Защита данных в распределенных системах | | | | | | | | | |
|  | | | | | |  | | |  | |
|  | 6.1 Распределенные вычислительные среды | | | | | | | | | |
|  | Распределенная обработка информации в среде клиент-сервер. Концепция распределенной вычислительной среды Distributed Computing Environment (DCE). Распределенные базы данных в сетях ЭВМ. | | | | | | | | | |
|  | 6.2 Угрозы безопасности распределенных СУБД | | | | | | | | | |
|  | Угрозы доступности, целостности и конфиденциальности данных. Механизмы противодействия. | | | | | | | | | |
|  | 6.3 Распределенная обработка данных | | | | | | | | | |
|  | Понятие распределенной транзакции. Модель обработки транзакций. Мониторы обработки транзакций. Корпоративная среда обработки транзакций. | | | | | | | | | |
|  | 6.4 Протоколы фиксации | | | | | | | | | |
|  | Протоколы фиксации. Защищенные протоколы фиксации. Обработка распределенных транзакций в базах данных с многоуровневой секретностью (MLS). | | | | | | | | | |
|  | 6.5 Тиражирование данных | | | | | | | | | |
|  | Обзор средств тиражирования данных. Эффективные алгоритмы тиражирования. Сравне-ние подходов к тиражированию БД. | | | | | | | | | |
|  | 6.6 Интеграция БД и Internet | | | | | | | | | |
|  | Современные тенденции. Обзор существующих технологий. Вопросы безопасности: угрозы и методы противодействия. Перспективы развития. | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
|  | 7. Безопасность в статистических БД. | | | | | | | | | |
|  | | | | | |  | | |  | |
|  | 7.1. Общие сведения. | | | | | | | | | |
|  | Определение статистической БД. Классификация статистических БД. Характеристики статистических БД. | | | | | | | | | |
|  | 7.2. Угрозы статистических БД | | | | | | | | | |
|  | Статистический вывод. Виды компрометации статистических БД.. Методы получения информации из статистических БД. | | | | | | | | | |
|  | 7.3. Защита в статистических БД | | | | | | | | | |
|  | Методы защиты от вывода. Статистические фильтры. Статистические функции. Чувствительные статистики. Критерии сравнения методов защиты. | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
|  | 8. Распознавание вторжений в БД | | | | | | | | | |
|  | | | | | |  | | |  | |
|  | 8.1. Основные понятия. | | | | | | | | | |
|  | Определение понятия распознавания вторжений. Цели выявления злоупотреблений. Место процедуры распознавания вторжений в общей системе защиты. | | | | | | | | | |
|  | 8.2. Системы распознавания вторжений | | | | | | | | | |
|  | Типы моделей систем распознавания вторжений (ID-систем). Общая структура ID-систем. Шаблоны классов пользователей. Модели известных атак. | | | | | | | | | |
|  | 8.3. Экспертные ID-системы. | | | | | | | | | |
|  | Метрики. Статистические модели. Профили. Примеры ID-систем. | | | | | | | | | |
|  | 8.4. Развитие систем распознавания вторжений. | | | | | | | | | |
|  | Основные тенденции. | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
|  | 9. Проектирование безопасности БД. | | | | | | | | | |
|  | | | | | |  | | |  | |
|  | 9.1. Основные понятия | | | | | | | | | |
|  | Безопасное программное обеспечение. Правила безопасности. | | | | | | | | | |
|  | 9.2. Методология проектирования. | | | | | | | | | |
|  | Отличия в проектировании безопасных ОС и СУБД. Основные требования к безопасности СУБД. Независимые принципы целостности данных. Модель авторизации в System R. Архитектура безопасной СУБД. Архитектура SeaView и ASD. | | | | | | | | | |
|  | 9.3. Проектирование безопасных БД. | | | | | | | | | |
|  | Фазы проектирования безопасных БД (по DoD). Предварительный анализ. Требования и политики безопасности. Концептуальное проектирование. Логическое проектирование. Физическое проектирование. | | | | | | | | | |
|  | 9.4. Формальные верификации и спецификации. | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
| **5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)** | | | | | | | | | | |
|  | | | | | |  | | |  | |
|  | Компьютерный класс, мультимедийные проектор, аудиторная доска. | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
| **6. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины (модуля)** | | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
| Основная литература | | | | | | | | |  | |
|  | 1. Девянин П.Н. Модели безопасности компьютерных систем. – М.: "Academia", 2005 – 144 с. ISBN: 5-7695-2053-1  2. Терью М., Ньюмен А. Руководство по безопасности Oracle. Пер. с англ. – М.: Лори, 2004. – 560 с. ISBN 5-85582-220-6  3. Поляков А.М. Безопасность Oracle глазами аудитора: нападение и защита. М.: “ДМК Пресс” 2010. – 336 с. ISBN: 978-5-94074-517-4  4. Эриксон Д. Хакинг: искусство эксплойта. Пер. с англ. – М.: Символ-Плюс, 2005. – 240 с. ISBN 5-93286-076-6   5. К. Дж. Дейт Введение в системы баз данных = Introduction to Database Systems. — 8-е изд. — М.: «Вильямс», 2006. — С. 1328. — ISBN 0-321-19784-4 | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
| Дополнительная литература | | | | | | | | |  | |
|  | 1. Тоу Д. Настройка SQL для профессионалов: Пер. с англ. – СПб.: Питер, 2004. ISBN: 5-94723-959-0  2. Домарев В. Безопасность информационных технологий. Системный подход. – М.: Диа-Софт, 2004. – 992 с. ISBN 966-7992-36-5   3. Бармен С. Разработка правил информационной безопасности. – М.: Вильямс, 2002. – 208 с. ISBN 5-8459-0323-8   4. Мандиа К. Защита от вторжений. Расследование компьютерных преступлений. – М.: Лори, 2005. – 496 с. ISBN 5-85582-229-X  5. Миллсап К., Хольт Д. Oracle. Оптимизация производительности. – М.: Символ-Плюс, 2005. – 464 с. ISBN 5-93286-078-2 | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
| **7. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)** | | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
|  | На лекционных занятиях используются мультимедийные технологии, включая демонстрацию презентаций. Также ПО Microsoft Access | | | | | | | | | |
|  | Используется Case - средство разработки баз данных. | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
| **8. Методические указания для обучающихся по освоению дисциплины** | | | | | |  | | |  | |
|  |  |  |  |  |  |  | | |  | |
| Успешное освоение курса «Основы построения защищенных баз данных» требует большой самостоятельной работы студента. В программе курса приведено минимально необходимое время для работы студента над темой. | | | | | | | | | | |
| Самостоятельная работа включает в себя: | | | | | | | | | | |
| – чтение и конспектирование рекомендованной литературы, | | | | | | | | | | |
| – проработку учебного материала (по конспектам лекций, учебной и научной литературе); | | | | | | | | | | |
| – решение задач, предлагаемых студентам на лекциях, | | | | | | | | | | |
| – подготовку к контрольным, самостоятельным работам и тестам. | | | | | | | | | | |
|  | | | | | | | | | | |
| Руководство и контроль за самостоятельной работой студента осуществляется в результате анализа итогов контрольных, самостоятельных работ, а также индивидуальных консультаций. | | | | | | | | | | |
| Показателем владения материалом служит умение ставить и решать задачи. Для формирования умения применять теоретические знания на практике студенту необходимо решать как можно больше задач. | | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
| **9. Фонд оценочных средств для проведения промежуточной аттестации по итогам обучения** | | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
| Приложение | |  |  |  |  |  | | |  | |
|  | | | | | | | | | | |
|  | | | | | | | | | | |
|  | | | | | | | | | | |
|  | | | | | | | | | | |
|  | **ПРИЛОЖЕНИЕ** | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
|  |  |  | | | |  | | | | |
|  |  |  |  |  |  |  | | |  | |
|  |  |  |  |  |  |  |  |  | |  |
| **ФОНД ОЦЕНОЧНЫХ СРЕДСТВ** | | | | | | | | | | |
| **ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ** | | | | | | | | | | |
| **ПО ДИСЦИПЛИНЕ** | | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
|  | | | | | | | | | | |
| **по направлению:** | | Компьютерная безопасность (специалитет) | | | | | | |  | |
| **профиль подготовки:** | | Безопасность распределенных компьютерных систем | | | | | | | | |
|  |  | Факультет радиотехники и кибернетики | | | |  | | |  | |
|  | | кафедра защиты информации | | | |  | | |  | |
| **курс:** | | 5 | | | |  | | |  | |
| **квалификация:** | | специалист | | | |  | | |  | |
|  |  |  |  |  |  |  | | |  | |
| Семестр, формы промежуточной аттестации: 10(Весенний) - Экзамен | | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
| **Разработчики:** | | | | | |  | | |  | |
|  |  |  |  |  |  |  | | |  | |
| А.А. Алтухов , ассистент | | | | | | | | | | |
| В.А. Конявский , д-р техн. наук, ассистент | | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
| **1. Компетенции, формируемые в процессе изучения дисциплины** | | | | | | | | | | |
| Освоение дисциплины направлено на формирование у обучающегося следующих общекультурных (ОК), общепрофессиональных (ОПК) и профессиональных (ПК) компетенций: | | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
| способность к самоорганизации и самообразованию (ОК-8); | | | | | | | | | | |
| способность производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение (ПК-17); | | | | | | | | | | |
| способность производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации (ПК-18); | | | | | | | | | | |
| способность использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач (ОПК-8); | | | | | | | | | | |
| способность понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации (ОПК-3). | | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
| **2. Показатели оценивания компетенций** | | | | | |  | | |  | |
|  |  |  |  |  |  |  | | |  | |
| В результате изучения дисциплины «Основы построения защищенных баз данных» обучающийся должен: | | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
| **знать:** | |  |  |  |  |  | | |  | |
| • особенности математических моделей и их влияние на разработку системы БД;  • изобразительные средства, используемые в моделировании БД;  • языки описания и манипулирования данными разных классов (QBE, SQL, элементы 4GL);  • технологии организации БД. | | | | | | | | | | |
| **уметь:** | |  |  |  |  |  | | |  | |
| • определить предметную область;  • спроектировать реляционную базу данных (определить состав каждой таблицы, типы полей, ключ для каждой таблицы);  • работать с современными программными средствами (Case);  • определить ограничения целостности, получать результатные данные в виде различном виде (ответов на запросы, экранных форм, отчетов). | | | | | | | | | | |
| **владеть:** | |  |  |  |  |  | | |  | |
| • навыками работы в среде современных СУБД;  • способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства;  • способностью оценивать свои достоинства и недостатки, определять пути и выбирать средства развития достоинств и устранения недостатков;  • способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечения требуемого уровня эффективности применения автоматизированных систем. | | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
| **3. Перечень типовых контрольных заданий, используемых для оценки знаний, умений, навыков** | | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
|  |  |  |  |  |  |  | | |  | |
| 1. Дать определение угрозы. Виды «нарушителей». | | | | | | | | | | |
| 2. Назвать основные угрозы информации в автоматизированных системах. | | | | | | | | | | |
| 3. Назвать основные элементы системы лицензирования и сертификации средств защиты информационных процессов. | | | | | | | | | | |
| 4. Составить порядок аттестация защищенных систем. | | | | | | | | | | |
| 5. Структуры в РФ, обеспечивающие лицензирование и сертификацию. | | | | | | | | | | |
| 6. Основные компоненты нормативной базы по защите информационных процессов в автоматизиро-ванных системах | | | | | | | | | | |
| 7. Основные положения Руководящего документа Гостехкомиссии по оценке защищенности автоматизированных систем. | | | | | | | | | | |
| 8. Основные стандарты по защите информации и информационных процессов. | | | | | | | | | | |
| 9. Автоматизированные информационные системы. Состав подсистем. | | | | | | | | | | |
| 10. Роль и место баз данных в автоматизированных информационных системах. | | | | | | | | | | |
| 11. Основные определения и понятия безопасности информационных систем и баз данных. | | | | | | | | | | |
| 12. Назвать основные аспекты защиты данных и приведите примеры. | | | | | | | | | | |
| 13. Угрозы безопасности информационных систем. | | | | | | | | | | |
| 14. Базовые концепции безопасности информационных процессов в автоматизированных системах. | | | | | | | | | | |
| 15. Требования к подсистемам аудита информационных процессов. | | | | | | | | | | |
| 16. Чем определяются гарантии безопасности ИП в автоматизированных системах. Уровни гарантий. Основные положения методологии анализа гарантий. | | | | | | | | | | |
| 17. Принципы управление конфигурацией. | | | | | | | | | | |
| 18. Принципы безопасной установки систем защиты информационных процессов. | | | | | | | | | | |
| 19. Принципы безопасной модернизации информационных процессов в автоматизированных системах. | | | | | | | | | | |
| 20. Основные принципы обеспечения информационной безопасности в автоматизированной системе. | | | | | | | | | | |
| 21. Назвать основные методы построения защищенных автоматизированных систем. | | | | | | | | | | |
| 22. Дать определение политики безопасности. Основные типы политики безопасности. | | | | | | | | | | |
| 23. Назвать основные модели безопасности. | | | | | | | | | | |
| 24. Дать определение монитора безопасности обращений. | | | | | | | | | | |
| 25. Привести примеры скрытых каналы передачи информации. | | | | | | | | | | |
| 26. Назвать основные методы идентификации и аутентификации. | | | | | | | | | | |
| 27. Как можно разграничить доступ? | | | | | | | | | | |
| 28. Основные процедуры настройки параметров безопасности в ОС Windows. | | | | | | | | | | |
| 29. Основные функции средств защиты от копирования. | | | | | | | | | | |
| 30. Принцип защиты программ от исследования. | | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
| **4. Критерии оценивания** | | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
| Оценка отлично (10) выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины, проявляющему интерес к данной предметной области, продемонстрировавшему умение уверенно и творчески применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений. | | | | | | | | | | |
| Оценка отлично (9) выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений. | | | | | | | | | | |
| Оценка отлично (8) выставляется студенту, показавшему систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, правильное обоснование принятых решений, с некоторыми недочетами. | | | | | | | | | | |
| Оценка хорошо (7) выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но недостаточно грамотно обосновывает полученные результаты. | | | | | | | | | | |
| Оценка хорошо (6) выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности. | | | | | | | | | | |
| Оценка хорошо (5) выставляется студенту, если он в основном знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач достаточно большое количество неточностей. | | | | | | | | | | |
| Оценка удовлетворительно (4) выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он освоил основные разделы учебной программы, необходимые для дальнейшего обучения, и может применять полученные знания по образцу в стандартной ситуации. | | | | | | | | | | |
| Оценка удовлетворительно (3) выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, допускающему ошибки в формулировках базовых понятий, нарушения логической последовательности в изложении программного материала, слабо владеет основными разделами учебной программы, необходимыми для дальнейшего обучения и с трудом применяет полученные знания даже в стандартной ситуации. | | | | | | | | | | |
| Оценка неудовлетворительно (2) выставляется студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных принципов и не умеет использовать полученные знания при решении типовых задач. | | | | | | | | | | |
| Оценка неудовлетворительно (1) выставляется студенту, который не знает основного содержания учебной программы дисциплины, допускает грубейшие ошибки в формулировках базовых понятий дисциплины и вообще не имеет навыков решения типовых практических задач. | | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
| **5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности** | | | | | | | | | | |
|  |  |  |  |  |  |  | | |  | |
| Экзамен проводится в виде опроса в устной форме. При проведении экзамена обучающемуся предоставляется 60 минут на подготовку. Во время проведения зачета обучающиеся могут пользоваться программой дисциплины. | | | | | | | | | | |