

Министерство науки и высшего образования Российской Федерации
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Курганский государственный университет»
(КГУ)

Кафедра «Безопасность информационных и автоматизированных систем»



УТВЕРЖДАЮ:

Первый проректор

Т.Р. Змызгова /

«20» сентября 2021 г.

Рабочая программа учебной дисциплины

**РАЗРАБОТКА И ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ
СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ**

образовательной программы высшего образования –
программа специалитета

10.05.03 Информационная безопасность автоматизированных систем

Специализация № 5 «Безопасность открытых информационных систем»

Формы обучения: очная

Курган 2021

Рабочая программа дисциплины «Разработка и эксплуатация автоматизированных систем в защищенном исполнении» составлена в соответствии с учебным планом по программе специалитета «Информационная безопасность автоматизированных систем» (Безопасность открытых информационных систем), утвержденным для очной формы «30» августа 2021 года.

Рабочая программа дисциплины одобрена на заседании кафедры «Безопасность информационных и автоматизированных систем» 29 сентября 2021 года, протокол № 2.

Рабочую программу разработал
канд. тех. наук, доцент

Д.И. Дик

Согласовано:

Заведующий кафедрой БИАС
канд. тех. наук, доцент

Д.И. Дик

Начальник
Управления
образовательной деятельности

С.Н. Сеницын

Специалист
по учебно-методической работе
Учебно-методического отдела

Г.В. Казанкова

1. ОБЪЕМ ДИСЦИПЛИНЫ

Всего: 10 зачетных единицы трудоемкости (360 академических часов)

Очная форма обучения

| Вид учебной работы | На всю дисциплину | Семестр | |
|---|---------------------------|--------------|----------------|
| | | 9 | 10 |
| Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе: | 150 | 60 | 90 |
| Лекции | 60 | 30 | 30 |
| Лабораторные работы | 30 | - | 30 |
| Практические занятия | 60 | 30 | 30 |
| Самостоятельная работа, всего часов в том числе: | 210 | 84 | 126 |
| Курсовой проект | 36 | - | 36 |
| Подготовка к зачету | 18 | 18 | - |
| Подготовка к экзамену | 27 | - | 27 |
| Другие виды самостоятельной работы (подготовка к практическим и лабораторным работам, рубежному контролю) | 129 | 66 | 63 |
| Вид промежуточной аттестации | зачет, экзамен | зачет | экзамен |

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Разработка и эксплуатация автоматизированных систем в защищенном исполнении» относится к базовым дисциплинам Блока 1.

Изучение дисциплины базируется на результатах обучения, сформированных при изучении следующих дисциплин:

- Основы управленческой деятельности;
- Основы теории защиты информации;
- Основы информационной безопасности;
- Методы и средства криптографической защиты информации;
- Безопасность сетей ЭВМ;
- Организация ЭВМ и вычислительных систем.

Результаты обучения по дисциплине применяются в ходе курсового проектирования и итоговой аттестации (дипломного проектирования).

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Целью дисциплины является изучение основных нормативно-правовых актов международного, федерального и ведомственного уровня, определяющих организационные и правовые аспекты в области информационной безопасности.

Задачи дисциплины: приобретение необходимых знаний по следующим направлениям:

знаний о современных защищенных автоматизированных информационных системах, практическими навыками разработки и эксплуатации автоматизированных информационных систем для решения различных классов задач в соответствии с требованиями по защите информации; помогает формированию у обучаемых научного подхода к осмыслению процессов обработки, хранения и передачи информации, организации защиты этих процессов.

Компетенции, формируемые в результате освоения дисциплины:

- Способен разрабатывать компоненты систем защиты информации автоматизированных систем (ОПК-11).

- способность организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем (ОПК-13);

- способность осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений (ОПК-14);

- способность разрабатывать и эксплуатировать системы защиты информации открытых информационных систем (ОПК-5.2).

В результате изучения дисциплины обучающийся должен:

знать:

- основные угрозы безопасности информации и модели нарушителя в автоматизированных системах (для ОПК-11);

- критерии оценки защищенности открытых информационных систем (для ОПК-5.2);

- методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем (для ОПК-13, ОПК-14);

уметь:

- применять универсальный язык моделирования в разработке автоматизированных систем (ОПК-13).

- разрабатывать модели нарушителей и оценивать угрозы информационной безопасности автоматизированных систем (для ОПК-11, ОПК-14);

- контролировать эффективность проектирования, разработки и внедрения автоматизированных и открытых информационных систем; (для ОПК-11, ОПК-13, ОПК-14, ОПК-5.2);

владеть:

- методами и технологиями проектирования, моделирования, исследования подсистем безопасности автоматизированных систем (для ОПК-11, ОПК-13);

- методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных и открытых информационных систем (для ОПК-5.2, ОПК-14).

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Учебно-тематический план. Очная форма обучения

| Рубеж | Номер темы | Наименование темы | Количество часов контактной работы с преподавателем | | |
|--------------------------|------------|--|---|----------------------|---------------------|
| | | | Лекции | Практические занятия | Лабораторные работы |
| 9 семестр | | | | | |
| Рубеж 1 | 1 | Основы проектирования информационных систем | 6 | - | - |
| | 2 | Методологии проектирования информационных систем | 8 | 8 | - |
| | | Рубежный контроль 1. Тестирование | - | 2 | - |
| Рубеж 2 | 3 | Определение требований к информационной системе | 8 | 18 | - |
| | 4 | Проектирование архитектуры информационных систем | 8 | | - |
| | | Рубежный контроль 2. Тестирование | - | 2 | - |
| Итого за семестр: | | | 30 | 30 | - |
| 10 семестр | | | | | |
| Рубеж 3 | 5 | Построение распределенных информационных систем | 4 | - | - |
| | 6 | Общие вопросы архитектуры корпоративных программных систем | 4 | 12 | 6 |
| | 7 | Объектные модели и реляционные базы данных | 4 | - | 6 |
| | | Рубежный контроль 3. Тестирование | - | 2 | - |

| | | | | | |
|---------|----|---|-----------|-----------|-----------|
| Рубеж 4 | 8 | Управление параллельными заданиями | 4 | - | 4 |
| | 9 | Сеансы и состояния | 4 | - | 4 |
| | 10 | Представление данных в Web | 4 | - | 4 |
| | 11 | Разработка защищенных информационных систем | 6 | 14 | 6 |
| | | Рубежный контроль 4. Тестирование | - | 2 | - |
| | | Итого за семестр: | 30 | 30 | 30 |
| | | Всего: | 60 | 60 | 30 |

4.2. Содержание лекционных занятий

Тема 1. Основы проектирования информационных систем.

Введение в проектирование информационных систем. Жизненный цикл автоматизированной системы. Процессы жизненного цикла по стандарту ISO/IEC 12207 (ГОСТ 12207). Модели жизненного цикла.

Модель зрелости процесса разработки программного обеспечения (Capability Maturity Model).

Множественность методологий разработки программного обеспечения. Критерии выбора методологии.

Тема 2. Методологии проектирования информационных систем.

Гибкие и «тяжеловесные» методологии. Экстремально программирование: основные практики и риски методологии.

Управленческий фреймворк Scrum: роли, артефакты, процессы. Управление продуктом в Scrum.

Проектирование информационных систем в крупных компаниях.

Тема 3. Определение требований к информационной системе.

Определение образа и границ проекта. Варианты использования и сценарии использования. Бизнес правила. Спецификация требований к информационной системе. Определение нефункциональных требований. Назначение приоритетов требований.

Тема 4. Проектирование архитектуры информационных систем.

Цели и задачи проектирования. Проблемы, связанные с проектированием программного обеспечения. Основные концепции проектирования. Методики проектирования. Паттерны проектирования.

Тема 5. Построение распределенных информационных систем.

Интеграция приложений. Типы интеграционных задач. Слабое связывание. Критерии интеграции приложений. Способы интеграции приложений: передача файла, общая база данных, удаленный вызов процедуры, обмен сообщениями.

Тема 6. Общие вопросы архитектуры корпоративных программных систем.

Развитие модели слоев в корпоративных программных приложениях. Три основных слоя. Многоуровневые приложения. Организация бизнес-логики. Уровень служб.

Тема 7. Объектные модели и реляционные базы данных.

Архитектурные решения. Функциональные проблемы. Считывание данных. Взаимное отображение объектов и реляционных структур.

Отображение связей. Наследование. Реализация отображения. Двойное отображение. Использование метаданных. Соединение с базой данных.

Тема 8. Управление параллельными заданиями.

Проблемы параллелизма. Контексты выполнения. Изолированность и устойчивость данных. Стратегии блокирования. Предотвращение возможности несогласованного чтения данных. Разрешение взаимоблокировок. Транзакции. ACID: свойства транзакций. Ресурсы транзакций. Уровни изоляции. Системные транзакции и бизнес-транзакции. Параллельные операции и серверы приложений.

Тема 9. Сеансы и состояния.

В чем преимущество отсутствия "состояния". Состояние сеанса. Способы сохранения состояния сеанса.

Тема 10. Представление данных в Web.

Типовые решения представлений. Типовые решения входных контроллеров.

Тема 11. Разработка защищенных информационных систем.

Жизненный цикл разработки защищенного программного обеспечения (Security Development Lifecycle).

Принципы построения защищенных приложений.

Моделирование опасностей. Процесс моделирования: декомпозиция системы, определение и классификация угроз, построение деревьев опасности, ранжирование опасностей.

Реакция на угрозы. Методы предотвращения угроз.

Тестирование защиты: декомпозиция системы; определения интерфейсов компонентов; упорядочение интерфейсов по степени уязвимости; определение структур данных, используемых каждым интерфейсом, тестирование защиты. Атака с иницированием мутации данных.

4.3. Практические занятия

| Номер темы | Наименование раздела, темы | Наименование тем практических занятий | Норматив времени, час. |
|-------------------------------|---|---|------------------------|
| 9 семестр | | | |
| 2 | Методологии проектирования информационных систем | Определение требований к системе с использованием Story mapping | 4 |
| | | Анализ сетевого трафика (Wireshark) | 4 |
| 3 | Определение требований к информационной системе | Построение диаграмм вариантов использования системы | 6 |
| | <i>1-ый рубежный контроль</i> | <i>Тестирование</i> | 2 |
| | Определение требований к информационной системе | Написание сценариев вариантов использования | 6 |
| | | Разработка спецификации требований к системе | 6 |
| <i>2-ой рубежный контроль</i> | <i>Тестирование</i> | 2 | |
| Итого за семестр | | | 30 |
| 10 семестр | | | |
| 6 | Общие вопросы архитектуры корпоративных программных систем. | Протоколы динамической маршрутизации | 6 |
| | | Настройки маршрутизаторов и маршрутизированных коммутаторов | 6 |
| | | <i>3-ий рубежный контроль</i> | <i>Тестирование</i> |

| | | | |
|-------------------------|---|--------------------------------|-----------|
| 11 | Разработка защищенных информационных систем | Изучение технологии NAT | 3 |
| | | Изучение работы IP сетей | 3 |
| | | Разработка сетевой архитектуры | 8 |
| | 4-ой рубежный контроль | Тестирование | 2 |
| <i>Итого за семестр</i> | | | 30 |
| <i>Всего</i> | | | 60 |

4.4 Лабораторные работы

| Номер темы | Наименование тем | Наименование тем лабораторных работ | Норматив времени, час. |
|-------------------------|---|---|------------------------|
| <i>10 семестр</i> | | | |
| 6-7 | Общие вопросы архитектуры корпоративных программных систем. Объектные модели и реляционные базы данных. | Построение диаграммы классов | 4 |
| | | Построение диаграммы последовательности | 4 |
| | | Построение коммуникационной диаграммы | 4 |
| 8-10 | Управление параллельными заданиями. Сеансы и состояния. Представление данных в Web. | Построение диаграммы состояния | 4 |
| | | Построение диаграммы деятельности | 4 |
| | | Построение диаграммы развертывания | 4 |
| 11 | Разработка защищенных информационных систем | Моделирование опасностей информационной системы | 6 |
| <i>Итого за семестр</i> | | | 30 |
| <i>Всего</i> | | | 30 |

4.5 Курсовой проект

Тема курсового проекта: «Проектирование защищенной прикладной информационной системы».

Целью курсового проекта является формирование навыков в спецификации и проектировании защищенных программных систем.

В рамках курсового проекта выполняется проектирование прикладной информационной системы. Тематика курсового проекта выбирается студентом самостоятельно и согласовывается с преподавателем.

В рамках курсового проекта студент должен решить следующие задачи:

- разработать спецификацию программной системы;
- произвести моделирование угроз информационной безопасности;
- произвести анализ рисков информационной безопасности;
- разработать архитектуру программной системы на языке UML.

К защите студентом предоставляется пояснительная записка к курсовому проекту, которая должна включать в себя:

- задание;
- общее описание системы;
- описание вариантов использования системы;
- описание функциональных требований к системе;
- описание прочих требований к системе;
- диаграммы потоков данных верхнего уровня;
- дерево опасностей информационной системы;
- оценку рисков информационной безопасности системы;
- модель базы данных системы;

– модель архитектуры системы (диаграмма классов, CRC карточки классов, диаграммы последовательности и кооперации для основных вариантов использования, диаграммы состояний или деятельности, при необходимости диаграммы компонентов и развертывания).

Объем пояснительной записки к курсовому проекту 20-25 страниц.

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

При прослушивании лекций рекомендуется в конспекте отмечать все важные моменты, на которых заостряет внимание преподаватель, в частности те, которые направлены на качественное выполнение соответствующей практической или лабораторной работы.

Залогом качественного выполнения практических и лабораторных работ является самостоятельная подготовка к ним накануне путем повторения материалов лекций. Преподавателем запланировано на практических и лабораторных работах коллективное взаимодействие и разбор конкретных ситуаций, а также обсуждение неясных моментов и ситуаций по лекционному курсу.

Для текущего контроля успеваемости преподавателем используется балльно-рейтинговая система контроля и оценки академической активности. Поэтому настоятельно рекомендуется тщательно прорабатывать материал дисциплины при самостоятельной работе, участвовать во всех формах обсуждения и взаимодействия, как на лекциях, так и на практических и лабораторных работах в целях лучшего освоения материала и получения высокой оценки по результатам освоения дисциплины.

Выполнение самостоятельной работы подразумевает самостоятельное изучение разделов дисциплины, выполнение курсового проекта, подготовку к практическим и лабораторным работам, к рубежным контролям, подготовку к экзамену и зачету.

Рекомендуемая трудоемкость самостоятельной работы представлена в таблице:

Рекомендуемый режим самостоятельной работы

| Наименование вида самостоятельной работы | Рекомендуемая трудоемкость, акад. час. |
|--|---|
| Самостоятельное изучение тем дисциплины: | 80 |
| Основы проектирования информационных систем | 21 |
| Методологии проектирования информационных систем | 21 |
| Определение требований к информационной системе | 21 |
| Проектирование архитектуры информационных систем | 2 |
| Построение распределенных информационных систем | 1 |
| Общие вопросы архитектуры корпоративных программных систем | 2 |
| Объектные модели и реляционные базы данных | 2 |
| Управление параллельными заданиями | 2 |
| Сеансы и состояния | 2 |

| | |
|---|------------|
| Представление данных в Web | 2 |
| Разработка защищенных информационных систем | 4 |
| Подготовка к практическим занятиям (по 1 часу на каждое занятие) | 26 |
| Подготовка к лабораторным работам (по 1 часу на каждое занятие) | 15 |
| Подготовка к рубежным контролям (по 2 часа на каждый) | 8 |
| Подготовка к зачету | 18 |
| Курсовой проект | 36 |
| Подготовка к экзамену | 27 |
| Всего: | 210 |

При реализации программы дисциплины «Разработка и эксплуатация автоматизированных систем в защищенном исполнении» используется сочетание традиционных видов учебной работы в виде аудиторных занятий, состоящих из лекционных, практических занятий и лабораторных работ, с методами и формами активизации познавательной деятельности студентов для достижения запланированных результатов обучения и формирования компетенций. Для этого на кафедре "Безопасность информационных и автоматизированных систем" разработаны соответствующие программные учебно-методические комплексы (УМК), в которые интегрированы дидактические средства и методические материалы, обеспечивающие сопровождение учебного процесса по всем видам занятий и работ по дисциплине.

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Перечень оценочных средств

1. Балльно-рейтинговая система контроля и оценки академической активности студентов в КГУ (для очной формы обучения)
2. Отчеты студентов по практическим занятиям.
3. Отчеты по лабораторным работам.
4. Банк тестовых заданий к рубежным контролям № 1, № 2, №3 и №4.
5. Курсовой проект.
5. Перечень вопросов к зачету и экзамену.

6.2. Система балльно-рейтинговой оценки работы студентов по дисциплине

| № | Наименование | Содержание | | | | | | |
|---|---|---|---------------------------------------|--------------------------------------|--------------------------------------|----------------------|----------------------|---------|
| 1 | Распределение баллов за семестры по видам учебной работы, сроки сдачи учебной работы (доводятся до сведения студентов на первом учебном занятии) | Распределение баллов | | | | | | |
| | | 9 семестр | | | | | | |
| | | Вид учебной работы: | Посещение лекций | Выполнение практической работы | | Рубежный контроль №1 | Рубежный контроль №2 | Зачет |
| | | Балльная оценка: | 1 _б x 15 = 15 _б | 7 _б x 5 = 35 _б | | 10 | 10 | 30 |
| | | 10 семестр | | | | | | |
| | | Вид учебной работы: | Посещение лекций | Выполнение лабораторной работы | Выполнение практической работы | Рубежный контроль №1 | Рубежный контроль №2 | экзамен |
| | | Балльная оценка: | 1 _б x 15 = 15 _б | 4 _б x 7 = 28 _б | 3 _б x 5 = 15 _б | 6 | 6 | 30 |
| | | Курсовой проект | | | | | | |
| | Качество пояснительной записки | Качество программной части | Ритмичность выполнения | Качество защиты | Всего | | | |
| | до 20 | до 20 | до 20 | до 40 | 100 | | | |
| 2 | Критерий пересчета баллов в традиционную оценку по итогам работы в семестре и зачета | 60 и менее баллов – неудовлетворительно; незачет; 61...73 – удовлетворительно; зачет; 74... 90 – хорошо; 91...100 – отлично | | | | | | |
| 3 | Критерии допуска к промежуточной аттестации, возможности получения автоматического зачета (экзаменационной оценки) по дисциплине, возможность получения бонусных баллов | <p>Для допуска к промежуточной аттестации (экзамену, зачету) студент должен набрать по итогам текущего и рубежного контроля не менее 50 баллов и должен выполнить все практические и лабораторные работы и курсовой проект (в 9 и 10 семестрах).</p> <p>Для получения зачета «автоматически» студенту необходимо набрать 61 балл</p> <p>Для получения экзаменационной оценки «автоматически» студенту необходимо набрать следующее минимальное количество баллов:</p> <p>- 68 баллов для получения «автоматически» оценки «удовлетворительно».</p> <p>По согласованию с преподавателем студенту, набравшему минимум 68 баллов, могут быть добавлены дополнительные (бонусные) баллы за активность на практических и лабораторных работах, активное участие в научной и методической работе, оригинальность принятых решений в ходе выполнения практических и лабораторных работ, за участие в значимых учебных и внеучебных мероприятиях кафедры и выставлена за экзамен «автоматически» оценка «хорошо» или «отлично».</p> | | | | | | |

| | | |
|---|--|--|
| 4 | <p>Формы и виды учебной работы для неуспевающих (восстановившихся на курсе обучения) студентов для получения недостающих баллов в конце семестра</p> | <p>В случае если к промежуточной аттестации (экзамену или зачету) набрана сумма менее 50 баллов, студенту необходимо набрать недостающее количество баллов за счет выполнения дополнительных заданий, до конца последней (зачетной) недели семестра. При этом необходимо проработать материал всех пропущенных практических и лабораторных работ.</p> <p>Формы дополнительных заданий (назначаются преподавателем):</p> <ul style="list-style-type: none"> - выполнение и защита пропущенных практических работ – до 7 и 4 баллов в 9 и 10 семестрах соответственно; - выполнение и защита пропущенных лабораторных работ – до 3 баллов; - прохождение рубежного контроля – до 10 и 6 баллов за каждый рубеж в 9 и 10 семестрах соответственно. <p>Ликвидация академических задолженностей, возникших из-за разности в учебных планах при переводе или восстановлении, проводится путем выполнения дополнительных заданий, форма и объем которых определяется преподавателем.</p> |
|---|--|--|

6.3. Процедура оценивания результатов освоения дисциплины

Рубежные контроли проводятся в форме письменного тестирования. Зачет и экзамен проводится в традиционной форме.

Перед проведением каждого рубежного контроля преподаватель прорабатывает со студентами основной материал соответствующих разделов дисциплины в форме краткой лекции-дискуссии.

На каждое тестирование при рубежном контроле студенту отводится 1 час. Варианты тестовых заданий для рубежных контролей №1 и №2 состоят из 10 вопросов, для рубежного контроля №3 и №4 из 6 вопросов в каждом. Каждый вопрос оценивается в 1 балл.

Преподаватель оценивает в баллах результаты тестирования каждого студента по количеству правильных ответов и заносит в ведомость учета текущей успеваемости. Билет для экзамена и зачета состоит из 2-х вопросов, каждый из которых оценивается в 15 баллов. Время, отводимое студенту на подготовку и ответ на билет составляет 1 астрономический час.

Результаты текущего контроля успеваемости, защиты курсового проекта, зачета и экзамена заносятся преподавателем, соответственно, в зачетную или экзаменационную ведомость, которая сдается в организационный отдел института в день зачета или экзамена, а также выставляются в зачетную книжку студента.

6.4. Примеры оценочных средств для рубежных контролей, зачета и экзамена

1-ый рубежный контроль

1. Скорость проекта в XP?

- 1) величина, изменяющаяся от итерации к итерации
- 2) величина, постоянная на протяжении всего проекта
- 3) средняя скорость работы команды над группой процессов

2. Для мониторинга протекания спринта в Scrum используется?

- 1) Burndown diagram

- 2) Story mapping
- 3) покер планирование

3. Покер планирование в Scrum используется для определения?

- 1) трудоемкости пользовательской истории (задачи)
- 2) важности задачи
- 3) крайнего срока реализации задачи

2-ой рубежный контроль

1. Для чего предназначена диаграмма вариантов использования (прецедентов)?

- 1) задает перечень состояний, в которых может находиться система
- 2) представляет функциональные возможности системы, проявляющиеся при взаимодействии ее с окружающей средой
- 3) описывает последовательность действий, которые необходимо выполнить для достижения заданной цели

2. Для чего используется вариант использования (прецедент) на диаграмме вариантов использования?

- 1) для показа того, что делает система, не определяя при этом, каким образом она это делает
- 2) для задания последовательности действий, с помощью которых система достигает заданных целей

3. Как отображается вариант использования (прецедент)?

- 1) в виде окружности
- 2) в виде пунктирной окружности
- 3) в виде эллипса
- 4) в виде пунктирного эллипса

3-ый рубежный контроль

1. Для каких целей используется стереотип?

- 1) для создания нового класса моделирующих элементов, который вводится в процессе моделирования
- 2) для акцентирования внимания на помеченном стереотипом элементе

2. Метод предотвращения возникновения конфликтов между параллельными бизнес транзакциями путем предоставления доступа к данным в конкретный момент времени только одной бизнес транзакции называется.

- 1) оптимистическая автономная блокировка
- 2) пессимистическая автономная блокировка
- 3) монопольная блокировка бизнес транзакции

3. Какой из методов формирования представления Web сайта позволяет использовать WYSIWYG редакторы для формирования внешнего вида страниц?

- 1) представление с преобразованием
- 2) представление по шаблону
- 3) представление по запросу

4-ой рубежный контроль

1. Какая из методик используется для классификации опасностей?

- 1) CLAMP
- 2) STRIDE
- 3) DREAD

2. Какой из языков моделирования используется для моделирования опасностей?

- 1) UML
- 2) диаграммы потоков данных
- 3) отношения сущность-связь

3. Какая из методик предложена Microsoft для оценки рисков при построении защищенных приложений?

- 1) CLAMP
- 2) STRIDE
- 3) DREAD

Примерный перечень вопросов к зачету

1. Жизненный цикл автоматизированной системы.
2. Процессы жизненного цикла.
3. Модели жизненного цикла.
4. Модель зрелости процесса разработки программного обеспечения (Capability Maturity Model).
5. Экстремально программирование: основные практики и риски методологии.
6. Управленческий фреймворк Scrum.
7. Диаграммы вариантов использования. Вариант использования. Действующее лицо. Отношения вариантов использования.
8. Описание сценариев вариантов использования.
9. Описание функциональных требований.
10. Таблица «событие реакция».
11. Спецификация требований.
12. Нефункциональные требования к системе.

Примерный перечень вопросов к экзамену

1. Жизненный цикл автоматизированной системы.
2. Процессы жизненного цикла.
3. Модели жизненного цикла.
4. Модель зрелости процесса разработки программного обеспечения (Capability Maturity Model)
5. Экстремально программирование: основные практики и риски методологии
6. Управленческий фреймворк Scrum
7. Диаграммы вариантов использования. Вариант использования. Действующее лицо. Отношения вариантов использования.

8. Описание сценариев вариантов использования.
9. Описание функциональных требований.
10. Таблица «событие реакция».
11. Спецификация требований
12. Нефункциональные требования к системе
13. Трехслойная архитектура. Ее преимущества. Распределение слоев по вычислительным узлам.
14. Представление бизнес-логики. Сценарий транзакции.
15. Представление бизнес-логики. Модель предметной области.
16. Представление бизнес-логики. Модуль таблицы.
17. Архитектурные типовые решения источников данных. Шлюз таблицы данных
18. Архитектурные типовые решения источников данных. Шлюз записи данных.
19. Архитектурные типовые решения источников данных. Активная запись.
20. Архитектурные типовые решения источников данных. Преобразователь данных.
21. Объектно-реляционные типовые решения, предназначенные для моделирования поведения. Единица работы.
22. Объектно-реляционные типовые решения, предназначенные для моделирования поведения. Коллекция объектов.
23. Объектно-реляционные типовые решения, предназначенные для моделирования поведения. Загрузка по требованию.
24. Объектно-реляционные типовые решения, предназначенные для моделирования структуры. Поле идентификации. Отображение внешних ключей.
25. Объектно-реляционные типовые решения, предназначенные для моделирования структуры. Отображение с помощью таблицы ассоциаций. Отображение зависимых объектов.
26. Объектно-реляционные типовые решения, предназначенные для моделирования структуры. Наследование с одной таблицей
27. Объектно-реляционные типовые решения, предназначенные для моделирования структуры. Наследование с таблицами для каждого класса
28. Объектно-реляционные типовые решения, предназначенные для моделирования структуры. Наследование с таблицами для каждого конкретного класса
29. Объектно-реляционные типовые решения, предназначенные для моделирования структуры. Преобразователи наследования
30. Типовые решения, предназначенные для представления данных в Web. Модель-представление-контроллер.
31. Типовые решения, предназначенные для представления данных в Web. Контроллер страниц.
32. Типовые решения, предназначенные для представления данных в Web. Контроллер запросов.

33. Типовые решения, предназначенные для представления данных в Web. Представление по шаблону.
34. Типовые решения, предназначенные для представления данных в Web. Представление с преобразованием.
35. Типовые решения, предназначенные для представления данных в Web. Двухэтапное представление.
36. Типовые решения для хранения состояния сеанса. Сохранение состояния сеанса на стороне клиента.
37. Типовые решения для хранения состояния сеанса. Сохранение состояния сеанса на стороне сервера.
38. Типовые решения для хранения состояния сеанса. Сохранение состояния сеанса в базе данных.
39. Общие механизмы расширения модели: сноски, ограничения, комментарии и стереотипы.
40. Пакеты: назначение и представление. Импортирование пакета. Утилиты.
41. Диаграммы статических структур: диаграмма классов и диаграмма объектов. Класс и его описание.
42. Представление атрибутов в классах.
43. Представление операций в классах.
44. Интерфейсы: назначение и представление.
45. Бинарная ассоциация. Класс ассоциации. Цель ассоциации. Множественность. Спецификатор ассоциации. Конгломерат и композиция.
46. N-арные ассоциации.
47. Обобщение. Зависимость.
48. Объект. Составные объекты. Связи.
49. Диаграмма последовательности. Линия жизни объекта. Активация. Сообщения. Время переходов.
50. Коммуникационные диаграммы. Кооперации. Роли коопераций. Мультиобъект. Сообщения на диаграммах коммуникации.
51. Диаграмма схем состояния. Состояние. Составные состояния.
52. События на диаграммах схем состояния. События изменения, сигнала, вызова и времени. Простые переходы.
53. Составные переходы. Переходы во вложенные состояния. Индикатор истории.
54. Диаграмма деятельности. Состояние действия, решения.
55. Компонентные диаграммы. Диаграммы развертывания.
56. Принципы проектирования безопасных программ
57. Классификация опасностей по методу STRIDE
58. Деревья опасностей (уязвимостей)
59. Методы предотвращения опасностей (устранения уязвимостей)
60. Методика оценка риска DREAD
61. Создание планов тестирования на основе модели опасностей
62. Методы возмущения среды (мутации данных) для обнаружения недостатков надежности

6.5. Фонд оценочных средств

Полный банк заданий для текущего, рубежных контролей и промежуточной аттестации по дисциплине, показатели, критерии, шкалы оценивания компетенций, методические материалы, определяющие процедуры оценивания образовательных результатов, приведены в учебно-методическом комплексе дисциплины.

7. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ УЧЕБНАЯ ЛИТЕРАТУРА

7.1 Основная литература:

1 Антамошкин, О.А. Программная инженерия. Теория и практика [Электронный ресурс] / О.А. Антамошкин. – Красноярск: СФУ, 2012. – 247 с. – Доступ из ЭБС «Консультант студента».

2 Руководство Microsoft по проектированию архитектуры приложений. Microsoft Patterns & Practices / Корпорация Майкрософт. – 2009. – 529 с. – Режим доступа: http://download.microsoft.com/documents/rus/msdn/ры_приложений_полная_книга.pdf, свободный. – Загл. с экрана.

3 Буч, Г. Язык UML. Руководство пользователя [Электронный ресурс] / Г. Буч, Д. Рамбо, И. Якобсон; Пер. с англ. Н. Мухин. – 2-е изд. – М.: ДМК Пресс, 2008. – 496 с. – Доступ из ЭБС «Консультант студента».

7.2 Дополнительная литература:

1 Шопырин Д.Г. Управление проектами разработки ПО: Учебно-методическое пособие по дисциплине "Гибкие технологии разработки программного обеспечения" / Д.Г. Шопырин. – СПб: СПбГУ ИТМО, 2007. – 131 с. – Режим доступа: <http://window.edu.ru/resource/373/60373>, свободный. – Загл. с экрана.

2 Скопин, И. Н. Основы менеджмента программных продуктов: курс лекций: учебное пособие: для студентов вузов/ И.Н. Скопин; Интернет-университет информационных технологий. – М.: Интернет-Университет информационных технологий, 2004. – 333 с. – (Основы информационных технологий). – ISBN 5-9556-0013-2 (в пер.)

3 Скопин, И. Н. Основы менеджмента программных продуктов [Электронный ресурс]: курс лекций: учебное пособие: для студентов вузов / И.Н. Скопин; Интернет-университет информационных технологий. – Электрон. дан. – М.: Интернет-Университет информационных технологий, 2004. – Режим доступа: <https://www.intuit.ru/studies/courses/38/38/info>, свободный. – Загл. с экрана.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

1. Дик, Д.И. Методические указания по выполнению лабораторных работ по дисциплине «Разработка и эксплуатация защищенных автоматизированных систем» программы специалитета 10.05.03 – Информационная безопасность автоматизированных систем [Электронный ресурс] / Д.И. Дик. – Электрон. текстовые дан. – Курган: КГУ, 2016. – 58 с.

2. Дик, Д.И. Моделирование опасностей [Электронный ресурс]: Методические указания по выполнению лабораторных работ по дисциплине «Разработка и эксплуатация защищенных автоматизированных систем» программы специалитета 10.05.03 – Информационная безопасность автоматизированных систем / Д.И. Дик. – Электрон. текстовые дан. – Курган: КГУ, 2016. – 32 с.

3. Дик, Д.И. Методические указания по выполнению практических занятий по дисциплине «Разработка и эксплуатация защищенных автоматизированных систем» программы специалитета 10.05.03 – Информационная безопасность автоматизированных систем [Электронный ресурс] / Д.И. Дик. – Электрон. текстовые дан. – Курган: КГУ, 2016. – 46 с.

4. Дик, Д.И. Проектирование защищенной прикладной информационной системы [Электронный ресурс]: Методические указания по выполнению курсового проекта по дисциплине «Разработка и эксплуатация защищенных автоматизированных систем» программы специалитета 10.05.03 – Информационная безопасность автоматизированных систем / Д.И. Дик. – Электрон. текстовые дан. – Курган: КГУ, 2016. – 21 с.

9. РЕСУРСЫ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1. Сайт дистанционного обучения в НОУ (Национальный Открытый Университет) «ИНТУИТ» содержит бесплатные курсы, программы повышения квалификации и профессиональной переподготовки, интересные доклады и другую полезную информацию <http://www.intuit.ru>.

2. Федеральный портал «Российское образование» <http://www.edu.ru/>

3. Информационный сайт, содержащий справочные материалы по информатике, которые включают в себя курс лекций, схемы, презентации, рефераты и др. informatikaplus.narod.ru

4. Сайт о высоких технологиях, новости индустрии из мира компьютерного «железа», тестовые испытания и обзоры оборудования IXBT.com.

5. Портал «Информационно-коммуникационные технологии в образовании» <http://www.ict.edu.ru>.

10. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

При чтении лекций используются слайдовые презентации.

Минимальные требования к операционной системе и программному обеспечению компьютера, используемого при показе слайдовых презентаций: Windows XP, Libre Office.

11. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Переносной проектор BENQ PB6110 с экраном, локальная сеть компьютеров на базе Intel Core i3-2120 - 16 шт. с выходом в Internet.

12. Для студентов, обучающихся с использованием дистанционных образовательных технологий

При использовании электронного обучения и дистанционных образовательных технологий (далее ЭО и ДОТ) занятия полностью или частично проводятся в режиме онлайн. Объем дисциплины и распределение нагрузки по видам работ соответствует п. 4.1. Распределение баллов соответствует п. 6.2 либо может быть изменено в соответствии с решением кафедры, в случае перехода на ЭО и ДОТ в процессе обучения. Решение кафедры об используемых технологиях и системе оценивания достижений обучающихся принимается с учетом мнения ведущего преподавателя и доводится до сведения обучающихся.

Аннотация к рабочей программе дисциплины
**«Разработка и эксплуатация автоматизированных систем в защищенном
исполнении»**

образовательной программы высшего образования –
программы специалитета

**10.05.03 – Информационная безопасность
автоматизированных систем**

Направленность:

Специализация № 5 «Безопасность открытых информационных систем»

Трудоемкость дисциплины: 10 з.е. (360 академических часа)

Семестр: 9 и 10 (очная форма обучения)

Форма промежуточной аттестации: зачет, экзамен

Содержание дисциплины

Основные проблемы проектирования программных средств. Разработка требований к программному обеспечению. Жизненный цикл разработки защищенных программных систем. Методологии разработки программных систем. Структурный и объектно-ориентированные подходы в проектировании ПО. Основные понятия унифицированного языка моделирования (UML). Диаграммы прецедентов, диаграммы классов, диаграммы взаимодействия, диаграммы последовательности, диаграммы состояний, компонентные диаграммы. Паттерны проектирования. Типовая архитектура корпоративных программных систем.