ПРИЛОЖЕНИЕ 1
к рабочей программе дисциплины

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ В.Ф. УТКИНА»

Кафедра «Информационная безопасность»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

по дисциплине

Б1.О.40 «Проектирование программного обеспечения систем защиты информации»

Направление подготовки – 10.05.00 «Информационная безопасность»

Специальность: 10.05.03 Информационная безопасность автоматизированных систем

Специализация: № 8 «Разработка автоматизированных систем в защищенном исполнении»

Квалификация выпускника – специалист

Форма обучения - очная

Рязань 2023 г.

1 ОБЩИЕ ПОЛОЖЕНИЯ

Оценочные материалы – это совокупность учебно-методических материалов (контрольных заданий, описаний форм и процедур), предназначенных для оценки качества освоения обучающимися данной дисциплины как части основной профессиональной образовательной программы.

Цель – оценить соответствие знаний, умений и уровня приобретенных компетенций, обучающихся целям и требованиям основной профессиональной образовательной программы в ходе проведения текущего контроля и промежуточной аттестации.

Основная задача – обеспечить оценку уровня сформированности общекультурных, общепрофессиональных и профессиональных компетенций, приобретаемых обучающимся в соответствии с этими требованиями.

Контроль знаний проводится в форме текущего контроля и промежуточной аттестации.

Текущий контроль успеваемости проводится с целью определения степени усвоения учебного материала, своевременного выявления и устранения недостатков в подготовке обучающихся и принятия необходимых мер по совершенствованию методики преподавания учебной дисциплины (модуля), организации работы обучающихся в ходе учебных занятий и оказания им индивидуальной помощи.

К контролю текущей успеваемости относятся проверка знаний, умений и навыков, приобретенных обучающимися в ходе выполнения индивидуальных заданий на практических занятиях и лабораторных работах. При оценивании результатов освоения практических занятий и применяется шкала оценки «зачтено – не зачтено». Количество практических работ и их тематика определена рабочей программой дисциплины.

Результат выполнения каждого индивидуального задания должен соответствовать всем критериям оценки в соответствии с компетенциями, установленными для заданного раздела дисциплины.

Промежуточный контроль по дисциплине осуществляется проведением теоретического зачета с оценкой.

2 ОПИСАНИЕ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ

Сформированность каждой компетенции (или ее части) в рамках освоения данной дисциплины оценивается по трехуровневой шкале:

1) пороговый уровень является обязательным для всех обучающихся по завершении освоения дисциплины;

2) продвинутый уровень характеризуется превышением минимальных характеристик сформированности компетенций по завершении освоения дисциплины;

3) эталонный уровень характеризуется максимально возможной выраженностью компетенций и является важным качественным ориентиром для самосовершенствования.

Уровень освоения компетенций, формируемых дисциплиной:

Описание критериев и шкалы оценивания тестирования:

Шкала оценивания	Критерий
3 балла (эталонный уровень)	уровень усвоения материала, предусмотренного программой: процент верных ответов на тестовые вопросы от 85 до 100%
2 балла (продвинутый уровень)	уровень усвоения материала, предусмотренного программой: процент верных ответов на тестовые вопросы от 70 до 84%
1 балл (пороговый уровень)	уровень усвоения материала, предусмотренного программой: процент верных ответов на тестовые вопросы от 50 до 69%
0 баллов	уровень усвоения материала, предусмотренного программой: процент верных ответов на тестовые вопросы от 0 до 49%

Описание критериев и шкалы оценивания теоретического вопроса:

Шкала оценивания	Критерий
3 балла (эталонный уровень)	выставляется студенту, который дал полный ответ на вопрос, показал глубокие систематизированные знания, смог привести примеры, ответил на дополнительные вопросы преподавателя
2 балла (продвинутый уровень)	выставляется студенту, который дал полный ответ на вопрос, но на некоторые дополнительные вопросы преподавателя ответил только с помощью наводящих вопросов
1 балл (пороговый уровень)	выставляется студенту, который дал неполный ответ на вопрос в билете и смог ответить на дополнительные вопросы только с помощью преподавателя
0 баллов	выставляется студенту, который не смог ответить на вопрос

Описание критериев и шкалы оценивания практического задания:

Шкала оценивания	Критерий
3 балла (эталонный уровень)	Задача решена верно
2 балла (продвинутый уровень)	Задача решена верно, но имеются неточности в логике решения
1 балл (пороговый уровень)	Задача решена верно, с дополнительными наводящими вопросами преподавателя
0 баллов	Задача не решена

На промежуточную аттестацию (зачет с оценкой) выносится тест (10 вопросов), два теоретических вопроса и 2 задачи. Максимально студент может набрать 15 баллов. Итоговый суммарный балл студента, полученный при прохождении промежуточной аттестации, переводится в традиционную форму по системе «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно».

Оценка «отлично» выставляется студенту, который набрал в сумме 15 баллов (выполнил все задания на эталонном уровне). Обязательным условием является выполнение всех предусмотренных в течение семестра практических заданий.

Оценка «хорошо» выставляется студенту, который набрал в сумме от 10 до 14 баллов при условии выполнения всех заданий на уровне не ниже продвинутого. Обязательным условием является выполнение всех предусмотренных в течение семестра практических заданий.

Оценка «удовлетворительно» выставляется студенту, который набрал в сумме от 5 до 9 баллов при условии выполнения всех заданий на уровне не ниже порогового. Обязательным условием является выполнение всех предусмотренных в течение семестра практических заданий.

Оценка «неудовлетворительно» выставляется студенту, который набрал в сумме менее 5 баллов или не выполнил всех предусмотренных в течение семестра практических заданий.

3 ПАСПОРТ ОЦЕНОЧНЫХ МАТЕРИАЛОВ ПО ДИСЦИПЛИНЕ

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или её части)/ индикатора	Вид, метод, форма оценочного мероприятия
1	Жизненный цикл ПО.	ОПК-8.2. (ОПК-8.2..1, ОПК-8.2..2, ОПК-8.2..3) ОПК-2(ОПК-2.1, ОПК-2.2)	зачет с оценкой
2	Построение моделей ПО.	ОПК-8.2. (ОПК-8.2..1, ОПК-8.2..2, ОПК-8.2..3) ОПК-2(ОПК-2.1, ОПК-2.2)	зачет с оценкой
3	Угрозы безопасности информации при разработке ПО.	ОПК-8.2. (ОПК-8.2..1, ОПК-8.2..2, ОПК-8.2..3) ОПК-2(ОПК-2.1, ОПК-2.2)	зачет с оценкой
4	Организационные и технические меры по разработке безопасного ПО, реализуемых на различных стадиях жизненного цикла разработки безопасного ПО.	ОПК-8.2. (ОПК-8.2..1, ОПК-8.2..2, ОПК-8.2..3) ОПК-2(ОПК-2.1, ОПК-2.2)	Зачет с оценкой
5	Выявление уязвимостей и НДВ в ПО.	ОПК-8.2. (ОПК-8.2..1, ОПК-8.2..2, ОПК-8.2..3) ОПК-2(ОПК-2.1, ОПК-2.2)	Зачет с оценкой
6	Методы анализа ПО.	ОПК-8.2. (ОПК-8.2..1, ОПК-8.2..2, ОПК-8.2..3) ОПК-2(ОПК-2.1, ОПК-2.2)	Зачет с оценкой

4 ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ

4.1. Промежуточная аттестация в форме зачета с оценкой

Код компетенции/ индикаторов	Результаты освоения ОПОП Содержание компетенций/индикаторов
ОПК-8.2. (ОПК-8.2..1, ОПК-8.2..2, ОПК-8.2..3)	Способен обеспечивать и осуществлять разработку проектных и организационных решений, документирование системы защиты информации автоматизированной системы в защищенном исполнении. ОПК-8.2..1 Готовит исходные данные и формирует требования к системе защиты информации автоматизированных систем в защищенном исполнении. ОПК-8.2..2 Осуществляет разработку проектных и организационных решений по системе защиты информации автоматизированных систем в защищенном исполнении. ОПК-8.2..3 Осуществляет документирование систем защиты информации автоматизированных систем защиты информации.

Типовые тестовые вопросы:

1. Для каких целей служит вариант использования на диаграмме вариантов использования:
- представляет класс предметной области;
+ описывает действия, совершаемые системой под воздействием актера;
- представляет объект заданного класса;
- описывает события в системе;
- передает сообщение между объектами системы.

2. Диаграмма классов используется для:
- описания функций системы;
+ представления классов системы и статических связей между ними;
- описания взаимодействия системы с внешними объектами;
- задания сервисов системы для актеров;
- описания последовательности событий в системе.

3. Как на диаграмме последовательности отображается время существования объекта в системе:
- функцией отсчета времени;
- фокусом активности;
+ линией жизни;
- временным интервалом между сообщениями;
- типом объекта.

4. Диаграмма кооперации показывает:
- совокупность объектов предметной области;
+ потоки данных между объектами;
- операции объектов;
- атрибуты объектов;
- наследование объектов.

5. Триггерный переход между состояниями срабатывает:
- при завершении do-деятельности;

- при завершении указанного интервала времени;
+ при наступлении события, внешнего по отношению к исходному состоянию;
- при выполнении заданного условия;
- при совпадении имени внешнего события и внутреннего действия.

6. Нетриггерный переход между состояниями срабатывает:
+ при завершении do-деятельности;
- при завершении указанного интервала времени;
- при наступлении события, внешнего по отношению к исходному состоянию;
- при выполнении заданного условия;
- при совпадении имени внешнего события и внутреннего действия.

7. Какая модель жизненного цикла подразумевает выполнение проекта без возможности возврата на предыдущие этапы:
+каскадная;
с промежуточным контролем;
спиральная;
инкрементальная.

8. Какая модель жизненного цикла является итерационной разновидностью каскадной модели:
каскадная;
+с промежуточным контролем;
спиральная;
инкрементальная.

9. Какая модель жизненного цикла основана на постепенном наращивании функционала с повторными уточнениями задач:
каскадная;
с промежуточным контролем;
+спиральная;
инкрементальная.

10. Какую модель жизненного цикла предпочтительнее использовать при большом количестве итераций:
каскадная;
с промежуточным контролем;
спиральная;
+инкрементальная.

Типовые практические задания:
Задание 1
В соответствии с вариантом разработать для заданной предметной области диаграмму вариантов использования и описательную спецификацию.

Критерии выполнения задания 1
Задание считается выполненным, если обучающийся определил варианты использования создаваемой системы и отношения между ними, а также назначил актеров, определяющих внешние подсистемы по отношению к создаваемой.

Задание 2
В соответствии с вариантом разработать для заданной предметной области диаграмму классов.

Критерии выполнения задания 2
Задание считается выполненным, если обучающийся выделил части предметной области задачи и представил каждую из них соответствующим классом с необходимыми атрибутами и операциями, а также определил отношения в иерархии классов.

Типовые теоретические вопросы:
1. Понятие проекта.
2. Планирование проектных задач.
3. Построение моделей ПО
4. Классификация моделей разрабатываемого ПО.
5. Проблемы разработки сложного ПО.
6. Язык UML. Диаграммы вариантов использования.
7. Язык UML. Диаграммы классов.
8. Язык UML. Диаграммы последовательности.
9. Язык UML. Диаграммы кооперации.
10. Язык UML. Диаграммы состояний.
11. Язык UML. Диаграммы деятельности.
12. Понятие жизненного цикла ПО.
13. Стандартизация процессов жизненного цикла ПО.
14. Виды процессов жизненного цикла.
15. Этапы разработки ИС.
16. Каскадная модель жизненного цикла ПО.
17. Поэтапная модель жизненного цикла ПО с промежуточным контролем.
18. Спиральная модель жизненного цикла ПО.
19. Инкрементальная модель жизненного цикла ПО.
20. Выбор жизненного цикла процесса разработки ПО.
21. Модель жизненного цикла при использовании технологии RUP.
22. Технология экстремального прогрпммирования XP.
23. Рабочие процессы RUP и диаграммы UML.
24. Методология быстрой разработки приложений RAD.
25. Технология визуального программирования.
26. Современные методологии создания ПО.

Код компетенции/ индикаторов	**Результаты освоения ОПОП Содержание компетенций/индикаторов**
ОПК-2 (ОПК-2.1, ОПК-2.2)	Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности. ОПК-2.1 Анализирует информационную инфраструктуру объектов профессиональной деятельности. ОПК-2.2 Выбирает основные защитные механизмы и средства обеспечения информационной безопасности объектов профессиональной деятельности

Типовые тестовые вопросы:

1. Безопасное программное обеспечение это:
+ программное обеспечение, разработанное с использованием совокупности мер, направленных на предотвращение появления и устранение уязвимостей;

программное обеспечение, прошедшее функциональное тестирование;
объектно-ориентированное программное обеспечение;
программное обеспечение на языках Java и C#.

2. Динамический анализ кода программы это:
+анализ кода программы в режиме непосредственного исполнения;
анализ условных переходов в программе;
анализ быстродействия программы;
анализ потоков программы.

3. Инструментальное средство это:
+компьютерная программа, используемая как средство разработки;
средство защиты информации;
описание процедур настройки и инсталляции;
средство анализа параметров сетевого трафика.

4. Тестирование на проникновение это:
+вид работ по выявлению уязвимостей программы, основанный на моделировании действий потенциального нарушителя;
тестирование программы на различных наборах входных данных;
вид нагрузочного тестирования;
сканирование уязвимостей.

5. Угроза безопасности информации это:
+совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации;
использование несертифицированных средств защиты информации;
использование устаревших версий программного обеспечения.

6. Уязвимость программы это:
+недостаток программы, который может быть использован для реализации угроз безопасности информации;
недостаточное быстродействие программы;
динамическое выделение программой оперативной памяти;
большое количество входных параметров.

7. Компьютерная атака это:
+целенаправленное несанкционированное воздействие на ресурс АСЗИ;
воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств АСЗИ;
совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации АСЗИ.

8. Сетевая атака это:
+компьютерная атака с использованием протоколов межсетевого взаимодействия;
попытка воздействия на веб-приложение;
попытка воздействия на клиент-серверное приложение;
попытка воздействия на серверную операционную систему.

9. Статический анализ исходного кода программы это:

+вид работ по инструментальному исследованию программы в режиме, не предусматривающем реального выполнения кода;
этап компиляции программы;
оптимизация исходного кода программы с целью повышения быстродействия.

10. Фаззинг-тестирование программы это:
+вид работ по исследованию программы, основанный на передаче программе случайных или специально сформированных входных данных, отличных от данных, предусмотренных алгоритмом работы программы;
выявление недекларированных возможностей;
проверка функций программы на соответствие техническому заданию;
вид нагрузочного тестирования.

11. Безопасность информации это:
+состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность;
обработка информации только сертифицированным программным обеспечением;
состояние информации при котором исключен несанкционированный доступ.

12. Защита информации это:
процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
+деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

Типовые практические задания:

Задание 3

Разработать описание структурно-функциональных характеристик автоматизированной системы библиотеки университета.

Критерий выполнения задания 3

Задание считается выполненным, если обучаемый выполнил описание структуры и функций системы в соответствии с методическими документами.

Задание 4

Разработать состав математического обеспечения АСЗИ бухгалтерии малого предприятия.

Критерии выполнения задания 4

Задание считается выполненным, если обучающийся в результате показал совокупность математических методов, моделей и алгоритмов, примененных в АСЗИ.

Задание 5

Разработать состав программного обеспечения АСЗИ бухгалтерии малого предприятия.

Критерии выполнения задания 5

Задание считается выполненным, если обучающийся в результате показал совокупность программ на носителях данных, программных документов, предназначенных для отладки, функционирования и проверки работоспособности АСЗИ.

Задание 6

Разработать состав информационного обеспечения АСЗИ бухгалтерии малого предприятия.

Критерии выполнения задания 6

Задание считается выполненным, если обучающийся в результате показал совокупность форм документов, классификаторов, нормативной базы, применяемой в АСЗИ при ее функционировании.

Задание 7

Разработать состав лингвистического обеспечения АСЗИ бухгалтерии малого предприятия.

Критерии выполнения задания 7

Задание считается выполненным, если обучающийся в результате показал совокупность средств и правил для формализации естественного языка, используемых при общении пользователей и эксплуатационного персонала автоматизированной системы с комплексом средств автоматизации при функционировании АСЗИ.

Типовые теоретические вопросы:

1. Основные термины и определения.
2. Порядок организации разработки видов АСЗИ.
3. Общие требования к технологической безопасности математического, программного, информационного, лингвистического обеспечения.
4. Инструментальные среды и средства разработки и анализа ПО.
5. ГОСТ 34.000-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.
6. ГОСТ Р 56939-2016 Защита информации. Разработка безопасного программного обеспечения.
7. ГОСТ Р 56546-2015 Классификация уязвимостей информационных систем.
8. ГОСТ Р 58412-2019 Защита информации. Разработка безопасного ПО. Угрозы безопасности информации при разработке ПО.
9. ГОСТ Р ИСО/МЭК 18045-2013 Методология оценки безопасности информационных технологий.
10. ГОСТ Р ИСО-МЭК 27034-1 Информационные технологии. Безопасность приложений. Часть 1. Безопасность приложений.
11. ГОСТ Р ИСО-МЭК 27034-7-2020 Информационные технологии. Безопасность приложений. Часть 7. Основы прогнозирования доверия.
12. Угрозы безопасности информации при разработке ПО (по ГОСТ Р 58412-2019).
13. Классификация уязвимостей информационных систем (по ГОСТ Р 56546—2015).
14. Выявление угроз безопасности информации при разработке ПО.
15. Оценка уровня доверия безопасности ПО (степени соответствия выявленной безопасности ПО предъявленным требованиям) (по ГОСТ Р ИСО-МЭК 27034-7).
16. Методы и средства оценки рисков информационной безопасности при создании ПО.
17. Общие требования к разработке математического обеспечения АСЗИ.
18. Общие требования к разработке программного обеспечения АСЗИ.
19. Общие требования к разработке информационного обеспечения АСЗИ.
20. Общие требования к разработке лингвистического обеспечения АСЗИ.

21. Общие требования к инструментальным средствам разработки программного и информационного обеспечения.

22. Требования по обеспечению информационной безопасности стенда для разработки программного и информационного обеспечения.

23. Требования к программно-методической документации в части информационной безопасности.

24. Меры по разработке безопасного ПО, реализуемые при выполнении анализа требований к ПО.

25. Меры по разработке безопасного ПО, реализуемые при выполнении проектирования архитектуры ПО.

26. Меры по разработке безопасного ПО, реализуемые при выполнении конструирования и комплексирования ПО.

27. Меры по разработке безопасного ПО, реализуемые при выполнении квалификационного тестирования ПО.

28. Меры по разработке безопасного ПО, реализуемые при выполнении инсталляции ПО и поддержки приемки ПО.

29. Меры по разработке безопасного ПО, реализуемые при решении проблем в программном обеспечении в процессе эксплуатации.

30. Меры по разработке безопасного ПО, реализуемые в процессе менеджмента документацией и конфигурацией программы.

31. Меры по разработке безопасного ПО, реализуемые в процессе менеджмента инфраструктурой среды разработки ПО.

32. Меры по разработке безопасного ПО, реализуемые в процессе менеджмента людскими ресурсами.

33. Виды тестирования ПО.

34. Статический анализ ПО.

35. Динамический анализ ПО.

36. Защита ПО от взлома и несанкционированного использования.

37. Угрозы и уязвимости информационной безопасности при разработке ПО.

38. Безопасное ПО.

39. Фаззинг.

40. Инструментальные среды и средства разработки и анализа ПО.

41. Управление конфигурацией ПО.

42. Документация разработчика ПО.

43. Цели создание безопасного ПО и меры по их достижению.