МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Ф. УТКИНА

Кафедра «Автоматизированные системы управления»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Специальность 01.03.02
«Прикладная математика и информатика»

ОПОП
«Программирование и анализ данных»

Квалификация выпускника – бакалавр

Формы обучения – очная

Рязань 2025

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, 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. При оценивании результатов освоения практических занятий применяется шкала оценки «зачтено – не зачтено». Количество практических работ и их тематика определена рабочей программой дисциплины, утвержденной заведующим кафедрой.

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 экзамена.

Форма проведения экзамена – устный ответ по утвержденным вопросам, сформулированным с учетом содержания учебной дисциплины. После устного ответа обучаемого производится оценка его ответа преподавателем по шкале «неудовлетворительно – удовлетворительно – хорошо – отлично» и, при необходимости, проводится теоретическая беседа с обучаемым для уточнения оценки.

2. Паспорт фонда оценочных средств по дисциплине

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или её части)	Вид, метод, форма оценочного мероприятия
1	2	3	4
1	Тема 1. Информационная безопасность (ИБ). Введение	ОПК-4.1–З ОПК-4.1–У ОПК-4.1–В ОПК-4.2–З ОПК-4.2–У ОПК-4.2–В	Экзамен
2	Тема 2. ИБ автоматизированных систем	ОПК-4.1–З ОПК-4.1–У ОПК-4.1–В ОПК-4.2–З ОПК-4.2–У ОПК-4.2–В	Экзамен
3	Тема 3. Меры обеспечения защиты информации	ОПК-4.1–З ОПК-4.1–У ОПК-4.1–В ОПК-4.2–З ОПК-4.2–У ОПК-4.2–В	Экзамен

Критерии оценивания компетенций (результатов)

1) Уровень усвоения материала, предусмотренного программой.

2) Умение анализировать материал, устанавливать причинно-следственные связи.

3) Ответы на вопросы: полнота, аргументированность, убежденность, умение.

4) Качество ответа (его общая композиция, логичность, убежденность, общая эрудиция).

5) Использование дополнительной литературы при подготовке ответов.

Оценка **«Отлично»** выставляется студенту, который:

− по результатам текущего контроля имеет уровень сформированности компетенций не ниже порогового;

− продемонстрировал всестороннее, систематическое и глубокое знание учебно-программного материала дисциплины, умение успешно выполнять задания, предусмотренные программой;

− усвоил основную и ознакомился с дополнительной литературой, рекомендованной программой.

Оценка «отлично» выставляется студентам, усвоившим взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии; способным исчерпывающе, последовательно, грамотно и логически стройно изложить теоретический материал, безупречно ответить на дополнительные вопросы в рамках рабочей программы дисциплины.

Оценка **«Хорошо»** выставляется студенту, который:

− по результатам текущего контроля имеет уровень сформированности компетенций не ниже порогового;

− продемонстрировал полное знание учебно-программного материала дисциплины, умение успешно выполнять предусмотренные программой задания;

− усвоил основную литературу, рекомендованную в программе.

Оценка «хорошо» выставляется студентам, показавшим систематический характер знаний по дисциплине и способным к их самостоятельному пополнению и обновлению в ходе дальнейшей профессиональной деятельности; продемонстрировавшим знание всех основных теоретических понятий.

Оценка **«Удовлетворительно»** выставляется студенту, который:

− по результатам текущего контроля имеет уровень сформированности компетенций не ниже порогового;

− продемонстрировал общее знание основного учебно-программного материала дисциплины в объеме, необходимом для дальнейшей учебы и предстоящей работы по специальности;

− справился с выполнением заданий, предусмотренных программой;

− ознакомился с основной литературой, рекомендованной программой.

Оценка «удовлетворительно» выставляется студентам, допустившим ошибки в ответе на экзамене, но обладающим необходимыми знаниями для их устранения под руководством преподавателя, либо способным ответить на дополнительные вопросы того же раздела дисциплины.

Оценка **«Неудовлетворительно»** выставляется студенту, который:

− по результатам текущего контроля имеет неудовлетворительный уровень сформированности компетенций;

− продемонстрировал незнание значительной части основного учебнопрограммного материала дисциплины;

− допустил принципиальные ошибки в выполнении предусмотренных программой заданий;

− показал отсутствие навыков в обосновании выдвигаемых предложений;

− допустил существенные ошибки при изложении учебного материала.

Оценка «неудовлетворительно» выставляется студентам, которые не могут продолжить обучение по данной образовательной программе или приступить к профессиональной деятельности без дополнительных занятий по соответствующей дисциплине, а также, если студент после начала экзамена отказался его сдавать или нарушил правила защиты (не самостоятельно работал, обманом пытался получить более высокую оценку и т.д.).

Типовые контрольные задания или иные материалы

Вопросы к экзамену по дисциплине

1. Понятие информации. Доступ к информации. Информационная безопасность (ИБ).
2. Информационные (ИС) и автоматизированные системы (АС).
3. Обработка и защита информации.
4. Доступность. Целостность. Конфиденциальность.
5. Информационная безопасность АСУ ТП.
6. Атаки на АСУ ТП. Примеры атак.
7. Пути проникновения в закрытые АСУ ТП.
8. Сравнение ИС и АС.
9. Уровни обеспечения ИБ АСУ ТП.
10. Угроза ИБ. Понятия: источник, уязвимость, угроза, несанкционированный доступ.
11. Угроза ИБ. Классификация угроз: по аспекту информационной безопасности.
12. Угроза ИБ. Классификация угроз: по компонентам объекта информатизации.
13. Угроза ИБ. Классификация угроз: по способу осуществления.
14. Угроза ИБ. Классификация угроз: по расположению источника угроз.
15. Источники угроз (антропогенные, техногенные, стихийные).
16. Примеры возможных угроз.
17. Комплексная защита информации.
18. Модели АСУ ТП и концепция обеспечения ИБ в АСУ ТП.
19. Требования к ИБ в АСУ ТП. Особенности обеспечения ИБ.
20. Нарушители безопасности информации. Модель нарушителя ИБ.
21. Тип нарушителей. Классификация нарушителей ИБ.
22. Потенциал нарушителей. Возможности нарушителей.
23. Виды и цели нарушителей.
24. Способы реализации угроз нарушителем.
25. Основные методы реализации угроз.
26. Модель угроз безопасности информации. Этапы создания модели.
27. Принципы обеспечения информационной безопасности.
28. Законодательные (правовые) меры защиты информации.
29. Стандарты информационной безопасности, нормативные документы, регулирующие информационную деятельность в РФ и мире.
30. Административные меры защиты информации.
31. Процедурные меры защиты информации.
32. Организационные меры защиты информации.
33. Физическая защита информации (сдерживание, обнаружение – задержка - реагирование).

34. Технические меры защиты информации. Аппаратные средства.

35. Технические меры защиты информации. Программные средства.

36. Технические меры защиты информации. Идентификация и аутентификация. Управление доступом к объектам.

37. Технические меры защиты информации. Ограничение программной среды.

38. Технические меры защиты информации. Защита машинных носителей информации. Регистрация событий безопасности.

39. Технические меры защиты информации. Антивирусная защита и обнаружение вторжений.

40. Технические меры защиты информации. Обеспечение целостности информационной системы и информации. Обеспечение доступности информации.

41. Технические меры защиты информации. Защита среды виртуализации, защита технических средств и защита информационной системы.

42. Криптографические методы защиты.

43. Стеганографические методы защиты.

44. Защита интеллектуальной собственности.

Практикум по дисциплине

№ п/п	Наименование практического занятия	Трудоемкость, час
1	Организационные меры защита информации	2
2	Управление доступом. Учётные записи пользователей	2
3	Управление доступом. Разграничение доступа к ресурсам в операционной системе	2
4	Управление доступом. Стойкость парольной защиты	2
5	Настройки параметров аудита в операционной системе	2
6	Обеспечение целостности и доступности данных	2
7	Криптография	2
8	Стеганография	2

Типовые задания для самостоятельной работы

1. Идентификация и аутентификация субъектов доступа и объектов доступа.
2. Управление доступом субъектов доступа к объектам доступа.
3. Ограничения программной среды.
4. Защита машинных носителей информации.
5. Регистрация событий безопасности.
6. Антивирусная защита и обнаружение вторжений.
7. Контроль (анализ) защищенности информации.

8. Обеспечение целостности информационной системы и информации.

9. Обеспечение доступности информации.

10. Защита среды виртуализации.

11. Защита технических средств.

12. Защита информационной системы, ее средств, систем связи и передачи данных.

13. Криптографические методы защиты.

14. Стеганографические методы защиты.

15. TSL/SSL шифрование.