ПРИЛОЖЕНИЕ

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное
учреждение высшего образования

РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ ИМЕНИ В.Ф. УТКИНА

Кафедра «Телекоммуникаций и основ радиотехники»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

по дисциплине

Б1.О.09 «Основы защиты информации в инфокоммуникационных системах»

Направление подготовки
11.04.02 «Инфокоммуникационные технологии и системы связи»

Профиль подготовки (специализации)
«Интеллектуальные системы и сети телекоммуникаций»

Уровень подготовки — магистратура

Квалификация (степень) выпускника – магистр

Форма обучения – очная

Рязань 2025

Оценочные материалы предназначены для оценки качества освоения студентами данной дисциплины как обязательной части дисциплины базовой ОПОП.

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

Основная задача – обеспечить оценку уровня сформированности компетенций, приобретаемых студентами в ходе изучения дисциплины и поддерживаемых ею.

Контроль знаний студентов 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 студентов и принятия необходимых мер по совершенствованию методики преподавания учебной дисциплины (модуля), организации работы студентов в ходе учебных занятий и оказания им индивидуальной помощи.

К текущему контролю относятся проверка знаний, умений и навыков студентов: на занятиях; по результатам выполнения самостоятельных работ, КР; по результатам тестирования в ходе семестра; по результатам выполнения обучающимися индивидуальных заданий; по результатам проверки качества конспектов лекций и иных материалов. При оценивании (определении) результатов освоения дисциплины применяется традиционная система (отлично, хорошо, удовлетворительно, неудовлетворительно) или двоичная система.

По итогам изучения дисциплины (промежуточная аттестация) студенты сдают зачет (в четвертом семестре), экзамен (в пятом семестре) и защищают курсовую работу (в пятом семестре). Форма проведения зачета и экзамена – письменный ответ, по утвержденным заведующим кафедрой экзаменационным билетам или по вопросам для зачета, список которых приводится ниже. В билет для зачета включается три вопроса, в экзаменационный билет - три вопроса по темам курса. Для уточнения степени понимания студентом материала экзаменатором задаются дополнительные вопросы. Завершающим этапом выполнения курсовой работы является индивидуальная защита каждым студентом выполненной работы.

Паспорт фонда оценочных средств по дисциплине

№ п/п	Контролируемые разделы (темы) дисциплины (результаты по разделам)	Код контролируемой компетенции (или ее части)	Вид, метод, форма оценочного мероприятия
1	2	3	4
1	Проблема защиты информации в телекоммуникационных системах. Анализ основных угроз	ОПК-2	Экзамен
2	Криптографические методы защиты информации.	ОПК-2	Экзамен
3	Методы обеспечения подлинности пользователей и сообщений.	ОПК-2	Экзамен
4	Обеспечение безопасности информации в мобильных системах телекоммуникаций.	ОПК-2	Экзамен
5	Практика сетевой защиты.	ОПК-2	Экзамен

Расписание аудиторных занятий, предэкзаменационных консультаций и экзаменов составляет диспетчерская служба учебного отдела, выставляет его на сайт РГРТУ и вывешивает на бумажном носителе, утвержденном проректором по учебной работе, в установленном месте.

Расписание текущих консультаций в течение семестра по лекционному материалу, темам, вынесенным для самостоятельного изучения студентами, и курсовой работе составляется лектором дисциплины по согласованию со студентами, подписывается им и вывешивается на бумажном носителе на доске объявлений кафедры.

Если студент в ходе семестра не выполнил часть предусмотренной программой дисциплины учебной работы или не прошел часть текущих контролирующих мероприятий, знание им этого материала проверяется в ходе сдачи зачета или экзамена во время промежуточной аттестации.

2. Критерии оценивания освоения компетенций (результатов)

1) Полнота усвоения материала, предусмотренного программой.
2) Глубина понимания материала, умение устанавливать причинно-

следственные связи.

3) Умение применять освоенный материал к ситуациям, которые не рассматривались в ходе учебного процесса.
4) Использование дополнительной литературы при изучении дисциплины.
5) Качество ответа (его общая композиция, логичность, убежденность, общая эрудиция).

Содержательная сторона и качество материалов, приведенных в отчетах студента по лабораторным работам, практическим занятиям.

Уровень знаний, умений и навыков по дисциплине оценивается в форме бальной отметки:

«Отлично» заслуживает студент, обнаруживший всестороннее, систематическое и глубокое знание учебно-программного материала, умение свободно выполнять задания, предусмотренные программой, усвоивший основную и знакомый с дополнительной литературой, рекомендованной программой. Как правило, оценка «отлично» выставляется студентам, усвоившим взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии.

«Хорошо» заслуживает студент, обнаруживший полное знание учебно-программного материала, успешно выполняющий предусмотренные в программе задания, усвоивший основную литературу, рекомендованную в программе. Как правило, оценка «хорошо» выставляется студентам, показавшим систематический характер знаний по дисциплине и способным к их самостоятельному пополнению и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности.

«Удовлетворительно» заслуживает студент, обнаруживший знания основного учебно-программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по специальности, справляющийся с выполнением заданий, предусмотренных программой, знакомый с основной литературой, рекомендованной программой. Как правило, оценка «удовлетворительно» выставляется студентам, допустившим погрешности в ответе на экзамене и при выполнении экзаменационных заданий, но обладающим необходимыми знаниями для их устранения под руководством преподавателя.

«Неудовлетворительно» выставляется студенту, обнаружившему пробелы в знаниях основного учебно-программного материала, допустившему принципиальные ошибки в выполнении предусмотренных программой заданий или не выполнившего учебный план по дисциплине. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение или приступить к профессиональной деятельности по окончании вуза без дополнительных занятий по соответствующей дисциплине.

Оценка «зачтено» выставляется студенту, который прочно усвоил предусмотренный программный материал; правильно, аргументировано ответил на все вопросы, с приведением примеров; показал глубокие

систематизированные знания, владеет приемами рассуждения и сопоставляет материал из разных источников: теорию связывает с практикой, другими темами данного курса, других изучаемых предметов; без ошибок выполнил практическое задание.

Дополнительным условием получения оценки «зачтено» могут стать хорошие успехи при выполнении самостоятельной и контрольной работы, систематическая активная работа на упражнениях.

Оценка «не зачтено» выставляется студенту, который не справился с 50% вопросов и заданий билета, в ответах на дополнительные вопросы допустил существенные ошибки.

3. Типовые контролирующие материалы

3.1. Вопросы к зачёту по дисциплине

1. Классификация систем мобильной радио связи (СМР).
2. Методы доступа к среде передачи в беспроводных сетях.
3. Стандартизация в области телекоммуникаций.
4. Модель взаимодействия открытых систем.
5. Транкинговые системы связи.
6. Протоколы транкинговой связи.
7. Стандарт TETRA/
8. Сотовые системы мобильной связи (ССМС).
9. Стандарты ССМС.
10. Структурная схема ССМС.
11. Разделение каналов в GSM.
12. Мобильная связь третьего поколения.
13. Взаимодействие сетей GSM и UMTS.
14. Системы персонального радиовызова.
15. Системы персональной спутниковой связи.
16. Свойства защищенной системы
17. Понятие информационной безопасности
18. Составляющие интегральной безопасности телекоммуникационных и информационно-вычислительных сетей.
19. Формулировка проблемы информационной безопасности.
20. Основные составляющие информационной безопасности.
21. Виды воздействия нарушителя на сеть передачи данных.
22. Определения и классификация угроз.
23. Угрозы доступности.
24. Угрозы целостности.
25. Основные угрозы конфиденциальности.
26. Причины утечки информации.
27. Виды утечки информации.
28. Каналы утечки информации.
29. Способы хищения абонентского телефонного трафика.

30. Стандартизация вопросов по ИБ на национальном уровне.
31. Структура рабочих органов подкомитета ISO / IEC JTC1/SC27 (МОС/МЭК ОТК/SC27)
32. Эталонная модель взаимосвязи открытых систем.
33. Основные направления работы международной организации по стандартизации.
34. Функции (сервисы) безопасности.
35. Механизмы безопасности.
36. Управление безопасностью.
37. Практическая защищенность.
38. Основные понятия и определения криптографических методов защиты информации.
39. Классификация криптографических методов.
40. Классификация шифров.
41. Шифры замены. Расшифровать слово БЪВЫДИЕПВРП. Ключевое слово ПЕТРАКОВ. K=5. m =31
42. Шифры сложной замены.
43. Биграммный шифр Плейфера.
44. Шифрование по маршрутам Гамильтона.
45. Шифрование с помощью аналитических преобразований.
46. Шифрующие таблицы Трисемуса.
47. Шифры перестановки.
48. Поточная система шифрования.
49. Комбинирование алгоритмов блочного шифрования.
50. Отечественный стандарт шифрования ГОСТ 28147-89.
51. Асимметричные алгоритмы шифрования.
52. Комбинированный метод шифрования.
53. Схема шифрования Полига Хеллмана.
54. Схема шифрования Эль Гамаля.
55. Алгоритм шифрования RSA.
56. Алгоритм шифрования DES.
57. Распределение ключей криптографического преобразования.
58. Схема обмена секретными ключами Диффи – Хеллмана.
59. Идентификация и аутентификация. Основные понятия. Классификация.
60. Простая аутентификация.
61. Строгая аутентификация: односторонняя, двухсторонняя, трехсторонняя
62. Строгая аутентификация, основанная на симметричных алгоритмах.
63. Строгая аутентификация, основанная на симметричных алгоритмах.
64. Строгая аутентификация на основе ключевых хэш-функций.
65. Аутентификация с нулевой передачей знаний.
66. Централизованная аутентификация.
67. Основные свойства и процедуры ЭЦП.
68. Алгоритм ЭЦП RSA.
69. Алгоритм ЭЦП Эль Гамаля.

70. Алгоритм ЭЦП DSA.
71. Отечественный стандарт цифровой подписи.
72. ЭЦП с дополнительными функциональными свойствами.
73. Построение и использование хеш-функций.
74. Ключевые функции хеширования.
75. Бесключевые функции хеширования.
76. Основные методы и типы закрытия речевых сообщений.
77. Тенденция развития систем закрытия речи.
78. Скремблирование во временной области.
79. Скремблирование в частотной области.
80. Аналоговое скремблирование – достоинства и недостатки.
81. Комбинация временного и частотного скремблирования.
82. Дискретизация речи с последующим шифрованием
83. Компьютерная стеганография.
84. Алгоритмы слепой подписи.
85. Функции межсетевых экранов.
86. Требования к межсетевым экранам.
87. Классификация межсетевых экранов.
88. Обеспечение безопасности информации в стандарте TETRA.
89. Аутентификация в стандарте TETRA.
90. Шифрование информации в стандарте TETRA.
91. Обеспечение секретности абонента в стандарте TETRA.
92. Обеспечение безопасности информации в стандарте GSM.
93. Аутентификация в стандарте GSM.
94. Шифрование информации в стандарте GSM.
95. Обеспечение секретности абонента в стандарте GSM.
96. Обеспечение секретности в процедуре корректировки местоположения.
97. Обеспечение секретности при обмене сообщениями между HLR, VLR, MSC.
98. Модуль подлинности абонента стандарта GSM.
99. Механизмы безопасности систем третьего поколения.

Составил
к.т.н., доцент кафедры ТОР П.Б. Никишкин

Зав. каф. ТОР,
д.т.н., профессор В. В. Витязев