МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Кафедра «Вычислительной и прикладной математики»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

по дисциплине

«ЗАЩИТА ИНФОРМАЦИИ»

Направление подготовки
09.03.01 «Информатика и вычислительная техника»

Направленность (профиль) подготовки
Системный анализ и инжиниринг информационных процессов
Системы автоматизированного проектирования вычислительных средств
Вычислительные машины, комплексы, системы и сети

Уровень подготовки
Бакалавриат

Квалификация выпускника – бакалавр

Форма обучения – очная, заочная

Рязань

1. Общие положения

Оценочные материалы – это совокупность учебно-методических материалов и процедур, предназначенных для оценки качества освоения обучающимися данной дисциплины как части основной образовательной программы.

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 общекультурных и профессиональных компетенций, приобретаемых обучающимся в соответствии с этими требованиями.

Контроль знаний обучающихся проводится в форме текущего контроля и промежуточной аттестации, итоговый контроль в форме зачета.

2. Паспорт оценочных материалов по дисциплине

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
	Раздел 1. Базовые понятия области защиты информации и безопасности информационных си-		
1.1	Проблема информационной безопасности общества. Основные термины и определения данной предметной области. Задачи по защите информации и информационных систем. Уровни формирования режима информационной безопасности. Обзор нормативно-правовых документов в области защиты информации. Государственные стандарты РФ – руководящие документы Гостехкомиссии России по защите информации. /Тема/		
1.2	Проблема информационной безопасности общества. Основные термины и определения данной предметной области. Задачи по защите информации и информационных систем. Уровни формирования режима информационной безопасности. Обзор нормативно-правовых документов в области защиты информации. Государственные стандарты РФ – руководящие документы Гостехкомиссии России по защите информации. Оценка рисков в сфере информационной безопасности. Основные методы средства, механизмы защиты информации. /Лек/	ОПК-3.2 ОПК-3.3	Зачет Практическая работа Лабораторная работа Самостоятельная работа

	Раздел 2. Угрозы информационной безопасности		
2.1	Исследование причин нарушения безопасности. Понятие угрозы информационной безопасности. Классификация угроз по различным классификационным признакам. Понятие уязвимости информации. Современные виды угроз. Понятие, виды, классификация, этапы реализации типовых сетевых атак. Технические каналы утечки информации. Каналы несанкционированного доступа к информации. /Тема/		
2.2	Исследование причин нарушения безопасности. Понятие угрозы информационной безопасности. Классификация угроз по различным классификационным признакам. Понятие уязвимости информации. Современные виды угроз. Понятие, виды, классификация, этапы реализации типовых сетевых атак. Технические каналы утечки информации. Каналы несанкционированного доступа к информации. /Лек/	ОПК-3.2 ОПК-3.3	Зачет Практическая работа Самостоятельная работа Контрольная работа
	Раздел 3. Общие подходы к проблеме защиты информации. Основные методы и средства защиты безопасности		
3.1	Общие подходы к проблеме защиты информации. Основные методы и средства защиты безопасности /Тема/		
3.2	Теоретические основы информационной безопасности. Понятия «объект», «субъект», «сущность», «процесс». Понятие модели безопасности. Виды моделей безопасности в зависимости от реализуемых функций защиты. Понятие политики безопасности. Мандатная, дискреционная, ролевая политики безопасности. /Лек/	ОПК-3.2 ОПК-3.3	Зачет Практическая работа Лабораторная работа Самостоятельная работа

3. Показатели и критерии оценивания компетенций (результатов) на различных этапах их формирования, описание шкал оценивания

Сформированность каждой компетенции в рамках освоения данной дисциплины оценивается по *трехуровневой шкале*:

- пороговый уровень (удовлетворительный) является обязательным для всех обучающихся по завершении освоения дисциплины;
- продвинутый уровень (хороший) характеризуется превышением минимальных характеристик сформированности компетенций по завершении освоения дисциплины;
- эталонный уровень (отличный) характеризуется максимально возможной выраженностью компетенций и является важным качественным ориентиром для самосовершенствования обучаемого.

При достаточном качестве освоения более 81% приведенных знаний, умений и навыков преподаватель оценивает освоение данной компетенции в рамках настоящей дисциплины на эталонном уровне, при освоении более 61% приведенных знаний, умений и навыков – на продвинутом, при освоении более 41% приведенных знаний умений и навыков – на пороговом уровне. При освоении менее 40% приведенных знаний, умений и навыков компетенция в рамках настоящей дисциплины считается неосвоенной.

Уровень сформированности каждой компетенции на различных этапах ее формирования в процессе освоения дисциплины оценивается в ходе текущего контроля успеваемости и представлено различными видами оценочных средств. Преподавателем оценивается содержательная сторона и качество устных и письменных ответов студентов на индивидуальные вопросы во время практических и лабораторных занятий, материалов, приведенных в письменном тестирование по теоретическим разделам курса и реферате. Дополнительным средством оценки знаний и умений студентов является отчет по проведенным лабораторным работам и их защита. Учитываются:

- уровень усвоения материала, предусмотренного программой курса;
- умение анализировать материал и устанавливать причинно-следственные связи;
- ответы на вопросы: полнота, аргументированность, убежденность, качество ответа (его общая композиция, логичность, общая эрудиция);
- качество выполненной лабораторной работы (программного продукта);
- правильность выполненной контрольной работы (теста);
- использование основной и дополнительной литературы при подготовке,
- и принимаются во внимание *знания, умения, навыки*, перечисленные в п.2. рабочей программы дисциплины.

Критерии оценивания уровня сформированности компетенции в процессе выполнения контрольных заданий:

41%-60% правильных ответов соответствует пороговому уровню сформированности компетенции на данном этапе ее формирования;

61%-80% правильных ответов соответствует продвинутому уровню сформированности компетенции на данном этапе ее формирования;

81%-100% правильных ответов соответствует эталонному уровню сформированности компетенции на данном этапе ее формирования.

Сформированность уровня компетенций не ниже порогового является основанием для допуска обучающегося к промежуточной аттестации по данной дисциплине. Формой промежуточной аттестации по данной дисциплине является зачет и экзамен, оцениваемые по принятой в ФГБОУ ВО «РГРТУ» системе.

Зачет оценивается по принятой в ФГБОУ ВО «РГРТУ» системе «зачтено» и «не зачтено»:

Шкала оценивания	Критерии оценивания
«зачтено»	*оценки «зачтено»* заслуживает обучающийся, продемонстрировавший полное знание материала дисциплины, усвоивший основную литературу, рекомендованную программой дисциплины; показавший систематический характер знаний, ответивший на все вопросы билета или допустивший погрешность в ответе, но обладающий необходимыми знаниями для ее устранения;
«не зачтено»	*оценки «не зачтено»* заслуживает обучающийся, не сдавший лабораторный практикум, продемонстрировавший серьезные пробелы в знаниях основного материала изученной дисциплины, не ответивший на все вопросы билета и дополнительные вопросы. Как правило, оценка «не зачтено» ставится обучающимся, которые не могут продолжить обучение по данной образовательной программе.

Экзамен оценивается по принятой в ФГБОУ ВО «РГРТУ» четырехбалльной системе: «неудовлетворительно», «удовлетворительно», «хорошо» и «отлично»:

Шкала оценивания	Критерии оценивания
«отлично»	*студент должен*: продемонстрировать глубокое усвоение материала; исчерпывающе, последовательно, грамотно и логически стройно изложить теоретический материал; правильно формулировать определения; уметь делать выводы по излагаемому материалу; безупречно ответить не только на вопросы билета, но и на дополнительные вопросы в рамках рабочей программы дисциплины; продемонстрировать умение правильно выполнять предусмотренные практические задания;
«хорошо»	*студент должен*: продемонстрировать достаточно полное знание материала; продемонстрировать знание основных теоретических понятий; достаточно последовательно, грамотно и логически стройно изложить материал; уметь сделать достаточно обоснованные выводы; ответить на все вопросы билета; продемонстрировать умение правильно выполнять практические задания, при этом возможны непринципиальные ошибки;
«удовлетворительно»	*студент должен*: продемонстрировать общее знание материала; знать основную рекомендуемую учебную литературу; уметь строить ответ в соответствии со структурой излагаемого вопроса; показать общее владение понятийным аппаратом дисциплины; уметь устранять допущенные ошибки в ответе на теоретические вопросы и при выполнении практических заданий, либо (при неправильном выполнении практического задания) по указанию преподавателя выполнить другие практические задания того же раздела дисциплины;
«неудовлетворительно»	*ставится в случае*: незнания значительной части программного материала; не владения понятийным аппаратом; существенных ошибок при изложении учебного материала; неумения строить ответ в соответствии со структурой излагаемого вопроса; неумения делать выводы. Как правило, такая оценка ставится студентам, которые не могут продолжить обучение по данной образовательной программе, а также, если студент после начала экзамена отказался его сдавать, или нарушил правила сдачи экзамена (списывал, подсказывал, обманом пытался получить более высокую оценку и т.д.).

. Типовые контрольные задания и иные материалы

4.1. Промежуточная аттестация (зачет)

Код компетенции	Содержание компетенции	Перечень планируемых результатов обучения по дисциплине
ОПК-3	**ОПК-3: Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности**	
ОПК-3.2	**Понимает основные требования информационной безопасности**	**Знать** принципы информационной и библиографической культуры, методы и средства решения стандартных задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. **Уметь** использовать принципы информационной и библиографической культуры, методы и средства решения стандартных задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. **Владеть** методами учета требований информационной безопасности.
ОПК-3.3	**Решает задачи профессиональной деятельности с применением информационно-коммуникационных технологий с учетом основных требований информационной безопасности**	**Знать** методы и средства решения стандартных задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. **Уметь** решать стандартные задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. **Владеть** методами и средствами решения стандартных задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

4.2. Темы практических занятий

Тема 1. Освоение приемов восстановления файлов, инфицированных вирусом, при отсутствии антивирусного программного обеспечения.

Тема 2. Основные принципы работы с электронной цифровой подписью.

Тема 3. Основные принципы работы алгоритма отечественной цифровой подписи «Нотариус»

Тема 4. Изучение стеганографического метода защиты информации от несанкционированного доступа.

4.3. Контрольные вопросы текущего контроля на практических занятиях и при защите лабораторных работ

1. Базовые понятия дисциплины «Информационная безопасность»
2. Дайте определение понятия «Информационная безопасность».
3. Дайте определение понятия «Защита информации».
4. Дайте определение понятия «Информация» с точки зрения информационной безопасности.
5. Назовите свойства информации, наиболее значимые с точки зрения

информационной безопасности.

6. Чем определяется уровень (степень) секретности информации или документа?
7. Что такое количественная характеристика информации, какие методы определения данной характеристики существуют?
8. Чем характеризуются прагматические свойства информации?
9. Дайте определение понятия «Информационная система».
10. Что понимают под информационным процессом?
11. Чем характеризуются информационные системы?
12. Что такое обработка информации в информационных системах?
13. Что такое физическая структура информационной системы?
14. Что такое логическая структура информационной системы?
15. Что такое топологическая структура информационной системы?
16. Что такое конфигурация информационной системы?
17. Что такое архитектура информационной системы?
18. Что такое информационный узел?
19. Что такое ресурсы информационной системы?
20. Кто считается пользователем информационной системы?
21. Какими критериями можно оценить качество информационной системы?
22. Что относится к средствам обеспечения информационных систем и их технологий?
23. Дайте характеристику распределённых информационных систем.
24. Какой структурный компонент системы понимается под объектом защиты?
25. Какой структурный компонент системы является элементом защиты?
26. Перечислите характеристики, влияющие на безопасность информации в информационной системе?
27. Дайте определение понятия «Угроза безопасности».
28. Дайте определение понятия «Уязвимость информации».
29. Что такое атака на информационную систему?
30. Что такое утечка информации?
31. Что такое разглашение информации?
32. Что такое несанкционированный доступ?
33. Дайте определение понятия «Политика безопасности»?
34. Какую угрозу информации представляют собой хакеры.
35. Что такое бесконтрольный уход информации?
36. Что такое канал утечки?
37. Назовите виды каналов утечки?
38. Назовите классификационные признаки угроз безопасности.
39. Какие виды угроз считаются умышленными, а какие непреднамеренными?
40. Что такое активные и пассивные угрозы?
41. Перечислите пути несанкционированного доступа к информации.
42. В чем особенности угроз и уязвимостей корпоративных сетей?
43. Перечислите виды атак в IP-сетях.
44. Перечислите наиболее общие проблемы безопасности информационных систем.
45. Перечислите основные группы методов и средств защиты информации.
46. Что входит в понятие комплексной защиты информации?
47. На какие виды подразделяются средства защиты информации?
48. Перечислите основные средства защиты информации.
49. Перечислите основные методы защиты информации.
50. Перечислите основные механизмы защиты информации.
51. Поясните содержание подходов к обеспечению безопасности информации и ин формационных систем, изложенные в межгосударственных стандартах информационной безопасности.

4.4. Типовые контрольные задания итогового контроля при проведении лабораторных работ

Задание 1.

Изучение методов криптографической защиты информации с использованием шифров перестановки.

1. ***Шифр маршрутной перестановки***
2. ***Шифр перестановки «Сцитала»***
3. ***Шифр «Поворотная решетка»***
4. ***Шифр вертикальной перестановки***
5. ***Шифр на основе магических квадратов***

Задание 2.

Изучение методов криптографической защиты информации с использованием шифров замены.

1. ***Шифр простой замены***
2. ***Шифр Цезаря***
3. ***Шифр «Аффинная система подстановок Цезаря»***
4. ***Шифр лозунговый***
5. ***Шифр «Полибианский квадрат»***
6. ***Шифрующая таблица Трисемуса***
7. ***Шифр биграммный Плейфера***
8. ***Шифрующая система омофонов***

Задание 3.

Изучение методов криптографической защиты информации с использованием шифров сложной замены.

1. ***Шифр Гронсфельда***
2. ***Система шифрования Вижинера***
3. ***Шифр Вижинера с автоключом***
4. ***Шифр Вижинера с перемешанным алфавитом***
5. ***Двойной квадрат Уитстона***

4.5. Типовые задания промежуточного контроля при выполнении контольных работ

Задание 4.

Изучение методов криптографической защиты информации путем проверки правильности ключа

Задание 5.

Шифрование методом гаммирования.

Задание 6.

Шифрование методом Вернама.

Задание 7.

Системы с открытым ключом. Алгоритм RSA

Задание 8.

Схема шифрования Полига – Хеллмана.

Задание 9.
Схема шифрования Эль-Гамаля.
Задание 10.

Шифрование с использованием потокового шифра RC4

4.6. Типовые задания для самостоятельной работы.

Тема 1. Проблемы защиты информационной системы. Защита для открытых информационных систем.
Тема 2. Характеристики, влияющие на безопасность информации.
Тема 3. Возможности сети Интернет и проблемы безопасности.
Тема 4. Угрозы и уязвимости корпоративных сетей и систем.
Тема 5. Задачи обеспечения информационной безопасности сетей.
Тема 6. Политика безопасности в сетях.
Тема 7. Технологии безопасности данных.
Тема 8. Использование комбинированной криптосистемы.
Тема 9. Строгая аутентификация.
Тема 10. Протокол Kerberos. (
Тема 11. Биометрическая аутентификация.
Тема 12. Типовые решения по применению межсетевых экранов для защиты информационных ресурсов.
Тема 13. Классификация сетей VPN.
Тема 14. Управление сетевой безопасностью.
Тема 15. Законодательный уровень информационной безопасности
Тема 16. Анализ текущего состояния российского законодательства в области информационной безопасности.
Тема 17. Методы управления средствами сетевой безопасностью
Тема 19. Задачи управления системой информационной безопасности предприятия
Тема 21. Освоение приемов противодействия разрушающим программным средствам.
Тема 22. Основные принципы работы с электронной цифровой подписью.
Тема 23. Основные принципы работы алгоритма отечественной цифровой подписи «Нотариус»

4.7. Вопросы итогового контроля (к зачету) по дисциплине

1. Введение. Сценарий безопасной работы информационной системы.
2. Все определения понятия «Информационная безопасность».
3. Составляющие информационной безопасности (ИБ).
4. Понятие предмета защиты.
5. Понятие объекта защиты.
6. Понятие комплексной системы защиты.
7. Системно-концептуальный подход к построению систем защиты.
8. Методы и средства построения ИБ. Их структура.
9. Виды собственного ПО системы ИБ.
10. Методы и средства обеспечения ИБ.
11. Основные средства защиты.
12. Методы, составляющие основу механизмов защиты.
13. Основные механизмы защиты.
14. Основные средства защиты от НСД.
15. Инженерно-технические средства защиты.
16. Методы и средства защиты от утечки по каналам ПЭМИН.
17. Методы и средства организационной защиты.
18. Основные понятия теории информационной безопасности.
19. Понятие информации как предмета защиты
20. Понятие информационного сервиса безопасности.
21. Свойства информации.
22. Законодательная база в сфере ИБ.
23. Статьи УК РФ в области ИБ.
24. Нормативно-правовые основы ИБ РФ.
25. Понятие тайны, виды тайн.
26. Понятие и свойства защищенной системы.
27. Информационные системы как объект защиты
28. Характеристики, влияющие на безопасность информации в информационной системе
29. Структура и состав основных компонентов информационных систем
30. Общие подходы к защите информации и информационных систем
31. Роль стандартов ИБ.
32. Международные стандарты ИБ.
33. Отечественные стандарты ИБ.
34. Особенности угроз в IP-сетях.
35. Основные виды угроз информационной безопасности.
36. Классификация угроз информационной безопасности.
37. Атаки на сеть. Сценарий проведения атак.
38. Виды атак, в IP-сетях
39. Понятие несанкционированного доступа к информации (НСД).
40. Виды НСД.
41. Основные виды разрушающих программных средств.
42. Каналы утечки информации. Технические каналы утечки информации.
43. Механизмов аутентификации и идентификации.
44. Функции и назначение межсетевых экранов.
45. Требования к межсетевым экранам.
46. Классификация межсетевых экранов.
47. Механизмы построения виртуальных защищенных сетей (VPN-технологии).
48. Защита интернет – подключений.

49. Защита системы электронной почты.
50. Разрушающие программные средства.
51. Вирусы. Основные понятия.
52. Классификация вирусов.
53. Криптография. Основные понятия.
54. Современные алгоритмы криптографии.
55. Понятие абсолютно стойкого шифра.
56. Классификация криптографических алгоритмов.
57. Понятие криптографии с открытым ключом.
58. Понятие электронной цифровой подписи (ЭЦП)
59. Понятие хэш-функции.
60. Основные алгоритмы ЭЦП, их различия.

Оператор ЭДО ООО "Компания "Тензор"
ДОКУМЕНТ ПОДПИСАН ПРОСТОЙ ЭЛЕКТРОННОЙ ПОДПИСЬЮ
СОГЛАСОВАНО, УТВЕРЖДЕНО, ПОДПИСАНО
ФГБОУ ВО "РГРТУ", РГРТУ, Борисов Василий Геннадьевич
Заведующий кафедрой ВПМ
10.09.26 08:28 (MSK)
Простая подпись