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 «Космические технологии»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

Б1.В.ДВ.02 «МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ»

Направление подготовки - 02.03.01 «Математика и компьютерные науки»

ОПОП академического бакалавриата «Математика и компьютерные науки»

Квалификация (степень) выпускника – бакалавр

Форма обучения - очная

Рязань 2022 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 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 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, приобретённых обучающимися на практических занятиях.

На практических занятиях допускается использование либо системы «зачтено – не зачтено», либо рейтинговой системы оценки, при которой, например, правильно решенная задача оценивается определенным количеством баллов. При поэтапном выполнении учебного плана баллы суммируются. Положительным итогом выполнения программы является определенное количество набранных баллов.

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.

Промежуточная аттестация студентов проводится на основании результатов выполнения ими ИДЗ, практических и лабораторных работ.

По итогам изучения разделов дисциплины «Методы и средства защиты информации», обучающиеся в конце учебного семестра проходят промежуточную аттестацию. Форма проведения аттестации – зачет в устной или письменной формах. Перечни вопросов, задач, примеров, выносимых на промежуточную аттестацию, составляются с учётом содержания тем учебной дисциплины.

В процессе подготовки к зачету экзаменуемый может составить в письменном виде план ответа, включающий в себя определения, выводы формулы, рисунки и т.п.

Паспорт фонда оценочных средств по дисциплине

Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или её части)	Вид, метод, форма оценочного мероприятия
1. Введение. Безопасность информации.	ПК-1	Зачет
2. Защита информации. Виды защиты информации.	ПК-1, ПК-4	Зачет
3. Объекты защиты информации.	ПК-1, ПК-4	Зачет
4. Защита информации в автоматизированных системах.	ПК-1, ПК-4	Зачет
5. Техническая защита информации.	ПК-1, ПК-4	Зачет
6. Контроль	ПК-1, ПК-4	Зачет

3. 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;

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

Перечень компетенций с указанием этапов их формирования

При освоении дисциплины «Методы и средства защиты информации» формируются компетенции: ПК-1 (индикаторы ПК-1.1), ПК-4 (индикаторы ПК-4.2).

Указанные компетенции формируются в соответствии со следующими этапами:

– формирование и развитие теоретических знаний, умений, навыков, предусмотренных данной компетенцией (лекционные занятия, самостоятельная работа студентов);

– приобретение и развитие практических знаний, умений, навыков, предусмотренных компетенцией (практические занятия, лабораторные работы, самостоятельная работа студентов);

закрепление теоретических знаний, умений, навыков, предусмотренных компетенцией, в ходе решения конкретных задач на практических занятиях, выполнения лабораторных работ, а также в процессе прохождения промежуточной аттестации.

Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Сформированность компетенции в рамках освоения данной дисциплины оценивается по двоичной шкале:

0 – компетенция не сформирована (выявляется менее 50% приведённых знаний, умений и навыков);

1 – компетенция сформирована (выявляется 50% и более приведённых знаний, умений и навыков).

Уровень сформированности компетенции на различных этапах её формирования в процессе освоения дисциплины «Методы и средства защиты информации» оценивается в ходе текущего контроля успеваемости и промежуточной аттестации и представлен различными видами оценочных средств.

Оценке сформированности в рамках данной дисциплины подлежат компетенции и индикаторы:

ПК-1: - Способен анализировать требования к программному обеспечению;

– ПК-1.1 - Анализирует возможности реализации требований к программному обеспечению;

ПК-4: Способен использовать современные методы разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования;

ПК-4.1 - Применяет пакеты прикладных программ моделирования.

Преподавателем оценивается содержательная сторона и качество изложения и аргументирования материалов на этапах промежуточной аттестации, итоги написания контрольной работы, ответы студента на вопросы по соответствующим видам занятий при текущем контроле на практических занятиях:

– контрольные опросы;
– контрольная работа;
– задания по практическим занятиям.

Принимается во внимание **знания** обучающимися:

– потенциальных угроз безопасности информации компьютерных систем;
– методов, средств и стандартов защиты информации.

наличие **умений**:

– определять угрозы безопасности информации и уязвимости компьютерных систем;
– определять средства и способы защиты информации в компьютерных системах.
–

обладание:

– навыками разработки требований к системе защиты информации компьютерных систем;
– навыками применения соответствующих мер защиты информации в компьютерных системах.

Критерии оценивания компетенций (результатов)

1. Уровень усвоения материала, предусмотренного программой.
2. Умение анализировать материал, устанавливать причинно-следственные связи.
3. Качество ответа на вопросы: полнота, аргументированность, убежденность, логичность.
4. Содержательная сторона и качество материалов, приведенных в отчетах студента по практическим занятиям.
5. Использование дополнительной литературы при подготовке ответов.

Формой промежуточной аттестации по дисциплине «Методы и средства защиты информации» является зачет с оценкой (в устной или письменной формах), оцениваемый по принятой в ФГБОУ ВО РГРТУ четырехбальной системе: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Критерии оценивания промежуточной аттестации представлены в таблице 1.

Таблица 1. Критерии оценивания промежуточной аттестации

Шкала оценивания	Критерии оценивания
«отлично»	**студент должен:** продемонстрировать глубокое и прочное усвоение знаний материала; исчерпывающе, последовательно, грамотно и логически стройно изложить теоретический материал; правильно формулировать определения; уметь сделать 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 практические задания, предусмотренные программой.
«хорошо»	**студент должен:** продемонстрировать достаточно полное знание материала; продемонстрировать знание основных теоретических понятий; достаточно последовательно, грамотно и логически стройно излагать материал; уметь сделать достаточно обоснованные выводы по излагаемому материалу; ответить на все вопросы билета; продемонстрировать умение правильно выполнять практические задания, предусмотренные программой, при этом возможно допустить непринципиальные ошибки.
«удовлетворительно»	**студент должен:** продемонстрировать общее знание изучаемого материала; знать основную рекомендуемую программой дисциплины учебную литературу; уметь строить ответ в соответствии со структурой излагаемого вопроса; показать общее владение понятийным аппаратом дисциплины; уметь устранить допущенные погрешности в ответе на теоретические вопросы и/или при выполнении практических заданий под руководством преподавателя, 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; невладения понятийным аппаратом дисциплины; существенных ошибок при изложении учебного материала; неумения строить ответ в соответствии со структурой излагаемого вопроса; неумения делать выводы по излагаемому материалу. Оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение по образовательной программе без дополнительных занятий по соответствующей дисциплине (формирования и развития

	компетенций, закрепленных за данной дисциплиной). Оценка «неудовлетворительно» выставляется также, если студент после начала экзамена отказался его сдавать или нарушил правила сдачи экзамена (списывал, обманом пытался получить более высокую оценку и т.д.).

4. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Для укрепления предусмотренных компетенциями, закреплёнными за дисциплиной знаниями, умениями и навыками, предусматривается текущая проверка путём опроса, выполнения заданий на практических занятиях, проверка знаний, умений и навыков, приобретаемых студентами самостоятельно, выполнения контрольной работы, проверка на промежуточной аттестации.

Фонд оценочных средств промежуточной аттестации, проводимой в форме зачета, включает: типовые теоретические вопросы; типовые практические вопросы; дополнительные вопросы.

Оценочные средства приведены ниже. Разрешается и иная формулировка вопроса или примера, без изменения его смысла или содержания, например, дробление, изменение условий или иное.

Вопросы к зачету

1. Информация. Безопасность информации.
2. Угрозы несанкционированного доступа к информации.
3. Состав и содержание угроз безопасности данных, обрабатываемых в компьютерных системах.
4. Общая классификация угроз безопасности информации.
5. Защита информации. Виды защиты информации.
6. Защита информации как деятельность.
7. Направления защиты информации.
8. Виды объектов защиты информации.
9. Информация как объект защиты.
10. Комплексные объекты защиты информации.
11. Автоматизированная система - комплексный объект защиты.
12. Угрозы информационной безопасности автоматизированных систем.
13. Определение актуальных угроз безопасности автоматизированных систем.
14. Модель нарушителя безопасности информации компьютерных систем.
15. Обеспечение безопасности компьютерных систем.
16. Методы и средства обеспечения безопасности компьютерных систем.
17. Меры обеспечения информационной безопасности создания компьютерных систем в защищенном исполнении.
18. Система защиты информации компьютерных систем.
19. Защита информационной системы от несанкционированного доступа.
20. Идентификация и аутентификация пользователей информационной системы.
21. Виды аутентификации.
22. Криптографическая защита информации.
23. Электронная цифровая подпись.
24. Объект информатизации как объект защиты информации.

25. Технические каналы утечки информации.
26. Виды технических каналов утечки информации.
27. Методы и средства технической защиты информации.
28. Активные способы защиты информации.
29. Основные организационно-технические мероприятия по защите информации.

Примеры типовых вопросов, соответствующих эталонному уровню сформированности компетенций

1. Информация. Безопасность информации.
2. Угрозы несанкционированного доступа к информации.
3. Состав и содержание угроз безопасности данных, обрабатываемых в компьютерных системах.
4. Общая классификация угроз безопасности информации.
5. Защита информации. Виды защиты информации.
6. Защита информации как деятельность.
7. Направления защиты информации.
8. Виды объектов защиты информации.
9. Информация как объект защиты.
10. Комплексные объекты защиты информации.
11. Автоматизированная система - комплексный объект защиты.
12. Угрозы информационной безопасности автоматизированных систем.
13. Определение актуальных угроз безопасности автоматизированных систем.
14. Модель нарушителя безопасности информации компьютерных систем.
15. Обеспечение безопасности компьютерных систем.
16. Методы и средства обеспечения безопасности компьютерных систем.
17. Меры обеспечения информационной безопасности создания компьютерных систем в защищенном исполнении.
18. Система защиты информации компьютерных систем.
19. Защита информационной системы от несанкционированного доступа.
20. Идентификация и аутентификация пользователей информационной системы.
21. Виды аутентификации.
22. Криптографическая защита информации.
23. Электронная цифровая подпись.
24. Объект информатизации как объект защиты информации.
25. Технические каналы утечки информации.
26. Виды технических каналов утечки информации.
27. Методы и средства технической защиты информации.
28. Активные способы защиты информации.
29. Основные организационно-технические мероприятия по защите информации.

Примеры типовых вопросов, соответствующих продвинутому уровню сформированности компетенций

1. Информация. Безопасность информации.
2. Угрозы несанкционированного доступа к информации.
3. Состав и содержание угроз безопасности данных, обрабатываемых в компьютерных системах.
4. Общая классификация угроз безопасности информации.
5. Защита информации. Виды защиты информации.
6. Защита информации как деятельность.
7. Направления защиты информации.
8. Виды объектов защиты информации.
9. Информация как объект защиты.
10. Комплексные объекты защиты информации.
11. Автоматизированная система - комплексный объект защиты.
12. Угрозы информационной безопасности автоматизированных систем.
13. Обеспечение безопасности компьютерных систем.
14. Методы и средства обеспечения безопасности компьютерных систем.
15. Меры обеспечения информационной безопасности создания компьютерных систем в защищенном исполнении.
16. Защита информационной системы от несанкционированного доступа.
17. Идентификация и аутентификация пользователей информационной системы.
18. Виды аутентификации.
19. Криптографическая защита информации.
20. Объект информатизации как объект защиты информации.
21. Технические каналы утечки информации.
22. Виды технических каналов утечки информации.
23. Методы и средства технической защиты информации.
24. Активные способы защиты информации.
25. Основные организационно-технические мероприятия по защите информации.

Примеры типовых вопросов, соответствующих пороговому уровню сформированности компетенций

1. Информация. Безопасность информации.
2. Угрозы несанкционированного доступа к информации.
3. Состав и содержание угроз безопасности данных, обрабатываемых в компьютерных системах.
4. Общая классификация угроз безопасности информации.
5. Защита информации. Виды защиты информации.
6. Защита информации как деятельность.
7. Направления защиты информации.
8. Виды объектов защиты информации.
9. Информация как объект защиты.
10. Комплексные объекты защиты информации.

11. Автоматизированная система - комплексный объект защиты.
12. Угрозы информационной безопасности автоматизированных систем.
13. Методы и средства обеспечения безопасности компьютерных систем.
14. Меры обеспечения информационной безопасности создания компьютерных систем в защищенном исполнении.
15. Защита информационной системы от несанкционированного доступа.
16. Идентификация и аутентификация пользователей информационной системы.
17. Виды аутентификации.
18. Криптографическая защита информации.
19. Электронная цифровая подпись.
20. Объект информатизации как объект защиты информации.
21. Технические каналы утечки информации.
22. Методы и средства технической защиты информации.
23. Основные организационно-технические мероприятия по защите информации.

План практических работ

1. Информация (определение). Виды информации. Безопасность информации (конфиденциальность, целостность, доступность). Угрозы безопасности информации.

2. Условия и факторы, создающие опасность несанкционированного, в том числе случайного, доступа к информации. Классификация угроз безопасности информации.

3. Защита информации как деятельность. Направления защиты информации. Защита информации от утечки. Защита информации от несанкционированного воздействия. Защита информации от непреднамеренного воздействия.

4. Автоматизированная система - комплексный объект защиты информации. Угрозы несанкционированного доступа к информации, обрабатываемой АС. Состав и содержание возможных источников и способов реализации угроз безопасности информации, обрабатываемой в автоматизированных системах.

5. Уязвимости информационных систем, причины их возникновения. Уязвимости программного обеспечения. Общая характеристика уязвимостей компьютерных систем. Классификация угроз безопасности информационных систем по используемой уязвимости. Уязвимости программного обеспечения КС.

6. Защита компьютерной системы от несанкционированного доступа к информации. Методы и средства защиты информации от несанкционированного доступа. Нарушители безопасности информации в автоматизированных системах. Возможности нарушителей.

7. Криптографическая защита информации в автоматизированных системах. Методы и средства защиты криптографической защиты информации в автоматизированных системах.

8. Объект информатизации - комплексный объект защиты информации. Технические каналы утечки информации. Определение технического канала утечки информации. Схема технического канала утечки информации. Электромагнитные и электрические каналы утечки информации. Способы и средства защиты.

Типовые задачи для практических занятий

Текущая проверка знаний, умений и навыков предусматривает в течение семестра периодические опросы и выполнение контрольной работы на практическом занятии. Контрольные опросы производятся на основании соответствующих типовых вопросов промежуточной аттестации. Варианты вопросов и контрольной работы приведены ниже.

Пример варианта типового вопроса

1. Информация. Безопасность информации, конфиденциальность, целостность, доступность.

Информация – сведения (сообщения, данные) независимо от формы их представления.

Безопасность информации – состояние защищенности информации, при котором обеспечивается ее конфиденциальность, целостность, доступность, а также другие заданные характеристики ее безопасности (подконтрольность, аутентичность и др.).

Конфиденциальность информации – защищенность информации от несанкционированного (не имеющего законного основания) получения;

Целостность информации – защищенность информации от несанкционированного (не имеющего законного основания) изменения;

Доступность информации – возможность своевременного санкционированного (имеющего законное основание) получения доступа к информации.

Оценочные материалы составлены в соответствии с рабочей программы дисциплины «Методы и средства защиты информации» по направлению подготовки 02.03.01 «Математика и компьютерные науки».

Составил
Ст. преподаватель кафедры
«Информационная безопасность» Н.А. Колесенков