ПРИЛОЖЕНИЕ 1

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Факультет вычислительной техники

Кафедра «Информационная безопасность»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДИСЦИПЛИНЫ

Б1.О.39 «Информационная безопасность автоматизированных систем»

Специальность: 10.05.03 Информационная безопасность автоматизированных систем

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

ОПОП по специальности: Информационная безопасность автоматизированных систем

Квалификация выпускника: специалист по защите информации

Форма обучения — очная
Срок обучения — 5,5 лет

Рязань 2023 г.

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 и практических занятий.

По итогам изучения разделов дисциплины «Информационная безопасность автоматизированных систем», обучающиеся в конце учебного семестра проходят промежуточную аттестацию. Форма проведения аттестации – зачет с оценкой 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

№ п/п	Контролируемые разделы (темы) дисциплины (результаты по разделам)	Код контролируемой компетенции (или её части)	Наименование оценочного средства
1	2	3	4
1	*1 раздел* Введение. Состав и содержание угроз безопасности информации в автоматизированных системах.	ОПК-8.1.1.	Практические занятия, зачет
2	*2 раздел* Виды угроз безопасности информации в автоматизированных системах.	ОПК-8.1.1.	Практические занятия, зачет
3	*3 раздел* Методы и средства обеспечения безопасности автоматизированных систем в защищенном исполнении.	ОПК-8.1 (ОПК-8.1.1, ОПК-8.1.2).	Практические занятия, зачет
4	*4 раздел* Нарушители безопасности информации в автоматизированных системах.	ОПК-8.1 (ОПК-8.1.1, ОПК-8.1.2).	Практические занятия, 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 «Информационная безопасность автоматизированных систем» формируются компетенции: ОПК-8.1 (индикаторы ОПК-8.1.1, ОПК-8.1.2).

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, самостоятельная работа студентов);

закрепление теоретических знаний, умений, навыков, предусмотренных компетенцией, в ходе решения конкретных задач на практических занятиях, 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 «Информационная безопасность автоматизированных систем» 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:

ОПК-8.1: Способен обосновывать целесообразность создания автоматизированной системы в защищенном исполнении и формировать исходные требования к этой системе, процессу ее создания и эксплуатации**.**

ОПК-8.1.1 - Проводит анализ угроз информационной безопасности при создании и эксплуатации автоматизированной системы в защищенном исполнении.

ОПК-8.1.2 - Формулирует и обосновывает требования информационной безопасности при создании и эксплуатации автоматизированной системы в защищенном исполнении.

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.

Принимается во внимание **знания** обучающимися:

– нормативных правовых актов по обеспечению режима секретности;

– нормативных и методических документов по выполнению режима защиты информации, в том числе ограниченного доступа.

наличие **умений**:

– организовать обеспечение режима секретности на объекте;

– выполнять работы по обеспечению информационной безопасности компьютерных систем;

– контролировать выполнения режима защиты информации, в том числе ограниченного доступа.

обладание:

– способами организации защиты информации ограниченного доступа;

– способами обеспечения информационной безопасности компьютерных систем;

– способами организации контроля защиты информации на объекте.

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 «Информационная безопасность автоматизированных систем» 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. Уязвимость.
2. Угрозы несанкционированного доступа к информации.
3. Состав и содержание угроз безопасности данных, обрабатываемых в автоматизированных системах.
4. Угрозы утечки информации по техническим каналам.
5. Угрозы утечки акустической (речевой) информации.
6. Угрозы утечки визуальной (видовой) информации.
7. Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок.
8. Уязвимость автоматизированных систем.
9. Общая характеристика уязвимостей автоматизированных систем.
10. Классификация угроз безопасности информационных систем по используемой уязвимости.
11. Общая классификация угроз безопасности информации автоматизированных систем.
12. Классификация угроз безопасности автоматизированных систем по виду защищаемой информации.
13. Классификация угроз безопасности автоматизированных систем по видам возможных источников угроз безопасности.
14. Классификация угроз безопасности автоматизированных систем по способам реализации угроз безопасности информации.
15. Обеспечение безопасности автоматизированных систем.
16. Методы и средства обеспечения безопасности.
17. Система защиты информации автоматизированных систем.
18. Меры обеспечения информационной безопасности создания автоматизированных систем в защищенном исполнении.

19. Модель нарушителя безопасности информации автоматизированных систем.
20. Общая характеристика источников угроз несанкционированного доступа в автоматизированных системах.
21. Угрозы безопасности информации, реализуемые с использованием протоколов межсетевого взаимодействия.
22. Угроза навязывания ложного маршрута сети.
23. Угрозы программно-математических воздействий.
24. Угрозы утечки информации по нетрадиционным информационным каналам.
25. Стеганографические каналы передачи информации.
26. Характеристика результатов несанкционированного или случайного доступа в автоматизированных системах.
27. Возможности нарушителя по реализации угроз безопасности информации в автоматизированных системах.
28. Модель нарушителя безопасности информации в автоматизированных системах.
29. Методика определения актуальных угроз безопасности автоматизированных систем.
30. Типовые модели угроз безопасности информации автоматизированных систем.
31. Анализ угроз безопасности информации автоматизированных систем.

Примеры типовых вопросов, соответствующих эталонному уровню сформированности компетенций

1. Информация. Безопасность информации. Уязвимость.
2. Угрозы несанкционированного доступа к информации.
3. Состав и содержание угроз безопасности данных, обрабатываемых в автоматизированных системах.
4. Угрозы утечки информации по техническим каналам.
5. Угрозы утечки акустической (речевой) информации.
6. Угрозы утечки визуальной (видовой) информации.
7. Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок.
8. Уязвимости автоматизированных систем.
9. Общая характеристика уязвимостей автоматизированных систем.
10. Классификация угроз безопасности автоматизированных систем по используемой уязвимости.
11. Общая классификация угроз безопасности информации автоматизированных систем.
12. Классификация угроз безопасности автоматизированных систем по виду защищаемой информации.
13. Классификация угроз безопасности информационных систем по видам возможных источников угроз безопасности.
14. Классификация угроз безопасности автоматизированных систем по способам реализации угроз безопасности информации.
15. Обеспечение безопасности автоматизированных систем.
16. Методы и средства обеспечения безопасности.
17. Система защиты информации автоматизированных систем.
18. Меры обеспечения информационной безопасности создания автоматизированных систем в защищенном исполнении.
19. Модель нарушителя безопасности информации автоматизированных систем.
20. Общая характеристика источников угроз несанкционированного доступа в автоматизированных системах.
21. Угрозы безопасности информации, реализуемые с использованием протоколов межсетевого взаимодействия.
22. Угроза навязывания ложного маршрута сети.
23. Угрозы программно-математических воздействий.
24. Угрозы утечки информации по нетрадиционным информационным каналам.
25. Стеганографические каналы передачи информации.
26. Характеристика результатов несанкционированного или случайного доступа в автоматизированные системы.
27. Возможности нарушителя по реализации угроз безопасности информации в автоматизированных системах.

28. Модель нарушителя безопасности информации в автоматизированных системах.
29. Методика определения актуальных угроз безопасности информации в автоматизированных системах.
30. Типовые модели угроз безопасности информации автоматизированных систем.
31. Анализ угроз безопасности информации автоматизированных систем.

Примеры типовых вопросов, соответствующих продвинутому уровню, сформированности компетенций

1. Информация. Безопасность информации. Уязвимость.
2. Угрозы несанкционированного доступа к информации.
3. Угрозы утечки информации по техническим каналам.
4. Уязвимость автоматизированных систем.
5. Общая характеристика уязвимостей автоматизированных систем.
6. Общая классификация угроз безопасности информации автоматизированных систем.
7. Классификация угроз безопасности автоматизированных систем по виду защищаемой информации.
8. Классификация угроз безопасности автоматизированных систем по видам возможных источников угроз безопасности.
9. Классификация угроз безопасности автоматизированных систем по способам реализации угроз безопасности информации.
10. Обеспечение безопасности автоматизированных систем.
11. Методы и средства обеспечения безопасности.
12. Меры обеспечения информационной безопасности создания автоматизированных систем в защищенном исполнении.
13. Модель нарушителя безопасности информации автоматизированных систем.
14. Общая характеристика источников угроз несанкционированного доступа в автоматизированных системах.
15. Угрозы безопасности информации, реализуемые с использованием протоколов межсетевого взаимодействия.
16. Угрозы программно-математических воздействий.
17. Характеристика результатов несанкционированного или случайного доступа в компьютерных систему.
18. Типовые модели угроз безопасности информации автоматизированных систем.

Примеры типовых вопросов, соответствующих пороговому уровню, сформированности компетенций

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

2. Угроза безопасности информации (определение).
3. Угрозы несанкционированного доступа к информации, общая характеристика.
4. Состав и содержание угроз безопасности данных, обрабатываемых в автоматизированных системах.
5. Уязвимости автоматизированных систем, причины их возникновения.
6. Общая характеристика уязвимостей автоматизированных систем.
7. Общая характеристика источников угроз несанкционированного доступа в автоматизированных системах.
8. Угрозы безопасности информации, реализуемые с использованием протоколов межсетевого взаимодействия.
9. Характеристика результатов несанкционированного или случайного доступа в автоматизированную систему.
10. Порядок определения актуальных угроз безопасности персональных данных в информационных системах персональных данных.
11. Обеспечение безопасности автоматизированных систем.
12. Методы и средства обеспечения безопасности.
13. Система защиты информации автоматизированных систем.
14. Меры обеспечения информационной безопасности создания автоматизированных систем в защищенном исполнении.

План практических занятий

1. Изучение классификации угроз безопасности информации автоматизированных систем по виду защищаемой информации.

Информация (определение). Безопасность информации (конфиденциальность, целостность, доступность). Угроза безопасности информации (определение). Условия и факторы, создающие опасность несанкционированного, в том числе случайного, доступа к информации АС. Классификация угроз безопасности автоматизированных систем.

2. Рассмотрение возможных источников и способов реализации угроз безопасности информации, обрабатываемой в автоматизированных системах.

Угрозы несанкционированного доступа к информации, обрабатываемой АС. Состав и содержание возможных источников и способов реализации угроз безопасности информации, обрабатываемой в автоматизированных системах. Характеристики АС, свойства среды (пути) распространения информативных сигналов, содержащих защищаемую информацию, возможности источников угрозы.

3. Уязвимости автоматизированных систем, причины их возникновения. Уязвимости программного обеспечения.

Общая характеристика уязвимостей автоматизированных систем.

Классификация угроз безопасности информационных систем по используемой уязвимости. Уязвимости программного обеспечения АС.

4. Угрозы нарушения доступности информации в АС, подключенном к сети общего пользования.

Угрозы безопасности АС, на базе автоматизированных рабочих мест, имеющих подключение к сетям связи общего пользования (однопользовательские). Угрозы, приводящие нарушению доступности информации - несанкционированному, в том числе случайному, воздействию на программные или программно-аппаратные элементы АС.

5. Угрозы программно-математических воздействий.

Введение в проблему вирусных угроз. Компьютерные вирусы.

Основная классификация компьютерных вирусов (по среде обитания: файловые загрузочные, макро, сетевые), их характеристики, особенности.

Жизненный цикл вирусов, хранение, исполнение.

6. Изучение угроз утечки информации по техническим каналам. Электромагнитные и электрические каналы утечки информации.

Определение технического канала утечки информации. Схема технического канала утечки информации. Электромагнитные и электрические каналы утечки информации.

7. Обеспечение безопасности автоматизированных систем. Методы и средства обеспечения безопасности.

8. Система защиты информации автоматизированных систем. Меры обеспечения информационной безопасности создания автоматизированных систем в защищенном исполнении.

9. Нарушители безопасности информации в автоматизированных системах. Построение модели внутреннего нарушителя безопасности информации АС.

Угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющих доступ к АС, включая пользователей, реализующих угрозы непосредственно в АС.

10. Нарушители безопасности информации в автоматизированных системах. Возможности нарушителей.

Построение модели внешнего нарушителя безопасности информации АС. Угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, не имеющих доступа к АРМ, реализующих угрозы из внешних сетей связи общего пользования.

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 (определение). 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.

Пример варианта контрольной работы

Разработка модели угроз безопасности информации автоматизированных систем.

Информация. Угроза безопасности информации. Уязвимость. Автоматизированные системы. Виды автоматизированных систем. АС ЗИ. Оценка условий реализации угроз безопасности информации АС. Источники угроз безопасности информации. Оценка возможностей нарушителей безопасности информации автоматизированных систем. Угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющих доступ к АС, включая пользователей, реализующих угрозы непосредственно в АС. Построение модели внутреннего нарушителя безопасности информации АС. Построение модели внешнего нарушителя безопасности информации АС.

Оценочные материалы составлены в соответствии с рабочей программы дисциплины «Информационная безопасность автоматизированных систем» по направлению подготовки 10.05.03 «Информационная безопасность автоматизированных систем».

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