МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ ИМЕНИ В.Ф. УТКИНА»

Кафедра «Государственного, муниципального и корпоративного управления»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

по дисциплине

Б1.В.ДВ.08.01 «Информационная безопасность»

Направление подготовки – 38.03.04 Государственное и муниципальное управление

Профиль – Информационные технологии в государственном и муниципальном управлении
ОПОП академического бакалавриата
«Государственное и муниципальное управление»

Квалификация выпускника – бакалавр
Формы обучения – заочная

Рязань 2020 г.

Оценочные материалы предназначены для контроля знаний обучающихся по дисциплине «Информационная безопасность» и представляют собой фонд оценочных средств, образованный совокупностью учебно-методических материалов (контрольных заданий для практических занятий), 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 образовательной программы в ходе проведения учебного процесса.

Основная задача – обеспечить оценку уровня сформированности общепрофессиональных и профессиональных компетенций, приобретаемых обучающимся в соответствии с этими требованиями.

Контроль знаний обучающихся 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 проведения, в случае необходимости, индивидуальных консультаций. К контролю текущей успеваемости относятся проверка знаний, умений и навыков, приобретённых обучающимися на лабораторных работах.

Промежуточная аттестация студентов по данной дисциплине проводится на основании результатов выполнения заданий на лабораторные работы. Количество лабораторных работ по дисциплине определено утвержденным учебным графиком.

По итогам курса студенты сдают в конце семестра обучения зачет. Форма проведения зачета – устный ответ, по утвержденному перечню вопросов, сформулированных с учетом содержания учебной дисциплины.

1. Паспорт фонда оценочных средств по дисциплине

№ п/п	Контролируемые разделы дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Понятие информационной безопасности. Основные составляющие	ОПК-1	Зачет
2	Объектно-ориентированный подход к рассмотрению защищаемых систем. Наиболее распространенные угрозы информационной безопасности и её составляющие	ОПК-1	Зачет
3	Законодательный уровень информационной безопасности. Административный уровень информационной безопасности	ОПК-1	Зачет
4	Процедурный уровень информационной безопасности	ОПК-1	Зачет
5	Основные характеристики программно-технических мер. Идентификация и аутентификация	ОПК-1, ПК-8	Лабораторная работа № 1 Зачет
6	Протоколирование и аудит, шифрование, контроль целостности.	ПК-8	Лабораторные работы № 2, 3 Зачет
7	Экранирование, анализ	ПК-8	Лабораторная работа № 4

	защищенности		Зачет
8	Обеспечение высокой доступности	ПК-8	Зачет

Критерии оценивания компетенций (результатов)

1. Уровень усвоения материала, предусмотренного программой.
2. Умение анализировать материал, устанавливать причинно-следственные связи.
3. Качество ответов на вопросы: логичность, убежденность, общая эрудиция.
4. Использование дополнительной литературы при подготовке ответов.
5. Умение вести поиск необходимой информации в сети Интернет.
6. Инициативность, умение работать в коллективе.
7. Качество оформления отчетной документации.

При аттестации результатов обучения по дисциплине в виде зачета используются следующие критерии.

«Зачтено»:

- студент не имеет на момент зачета задолженностей по лабораторным работам;
- студент ориентируется в представленных им отчетах о выполнении лабораторных работ, дает полные ответы на заданные по теме занятия вопросы.

«Не зачтено»:

- студент имеет на момент зачета задолженности по лабораторным работам;
- отсутствие осмысленного представления о существе вопроса, отсутствие ответов на заданные вопросы.

2 Примеры контрольных вопросов

1. Информационная безопасность. Защита информации, субъект информационных отношений, неприемлемый ущерб.
2. Доступность, целостность, конфиденциальность. Компьютерное преступление, жизненный цикл информационных систем.
3. Сложные системы. Структурный подход.
4. Основные определения и критерии классификации угроз.
5. Угроза, атака, уязвимость, окно опасности, источник угрозы, злоумышленник.
6. Основные угрозы доступности. Основные угрозы целостности. Основные угрозы конфиденциальности.
7. Российское законодательство в области информационной безопасности.
8. Зарубежное законодательство в области информационной безопасности.
9. Стандарты и спецификации в области информационной безопасности.
10. Основные понятия, политика безопасности.
11. Жизненный цикл информационной системы.
12. Синхронизация программы безопасности с жизненным циклом систем. Управление рисками.
13. Основные классы мер процедурного уровня.
14. Управление персоналом. Физическая защита.
15. Поддержание работоспособности.
16. Реагирование на нарушения режима безопасности.
17. Планирование восстановительных работ.
18. Основные понятия программно-технического уровня. Архитектурная безопасность.
19. Экранирование. Анализ защищённости.
20. Отказоустойчивость. Безопасное восстановление.
21. Основные понятия криптографии.
22. Парольная аутентификация. Одноразовые пароли. Сервер аутентификации Kerberos.

23. Идентификация/аутентификация с помощью биометрических данных.
24. Управление доступом. Ролевое управление доступом.
25. Активный аудит. Шифрование.
26. Симметричный метод шифрования.
27. Асимметричный метод шифрования.
28. Секретный и открытый ключ.
29. Криптография. Контроль целостности
30. Цифровые сертификаты.
31. Электронная цифровая подпись.
32. Экранирование. Фильтрация. Межсетевые экраны.
33. Классификация межсетевых экранов.
34. Архитектурная безопасность.
35. Транспортное экранирование. Анализ защищенности.
36. Сетевой сканер. Антивирусная защита.

3. Формы текущего контроля

Текущий контроль по дисциплине проводится в виде тестовых опросов по отдельным темам дисциплины, проверки заданий, выполняемых на лабораторных работах.

4. Формы промежуточного контроля

Промежуточный контроль по дисциплине – отчет о выполнении задания лабораторной работы, защита лабораторной работы.

5. Формы заключительного контроля

Форма заключительного контроля по дисциплине – зачет.

6. Критерий допуска к экзамену

К зачету допускаются студенты, выполнившие ко дню проведения зачета по расписанию зачетной недели все задания лабораторных работ.