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

КАФЕДРА ВЫЧИСЛИТЕЛЬНОЙ И ПРИКЛАДНОЙ МАТЕМАТИКИ

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

по дисциплине

Б1.О.25 «ЗАЩИТА ИНФОРМАЦИИ»

Направление подготовки

09.03.02 «Информационные системы и технологии»

ОПОП бакалавриата

«Информационные системы и технологии»

Квалификация (степень) выпускника – бакалавр

Формы обучения – очная, заочная

Рязань 2020

1. Общие положения

Оценочные материалы предназначены для контроля знаний обучающихся по дисциплине «Физические основы электротехники» и представляют собой фонд оценочных средств, образованный совокупностью учебно-методических материалов (контрольных заданий, описания критериев оценивания компетенций), 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 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 практических занятиях.

Практические занятия включают выполнение расчетов элекгических цепей по пройденным темам.

Промежуточная аттестация студентов по данной дисциплине проводится на основании результатов выполнения заданий для практических занятий и результатов выполнения контрольных работ. Количество практических занятий 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

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.

№ 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 систем.		
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

Критерии оценивания компетенций

1. Уровень усвоения материала, предусмотренного программой.
2. Умение анализировать материал, устанавливать причинно-следственные связи.
3. Качество ответов на вопросы: логичность, убежденность, общая эрудиция.

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

«Зачтено»:

- студент не имеет на момент зачета задолженностей по практическим занятиям;
- студент ориентируется в представленных им отчетах о выполнении заданий практического занятий, дает полные ответы на заданные по теме занятия вопросы.

«Не зачтено»:

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

2 Примеры контрольных вопросов для оценивания компетенций

ОПК-3.2

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?

ОПК-3.3

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?

Примеры задач
ОПК-3.2

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***

Варианты заданий

Для нечетных вариантов (1,3,…,25) предлагается реализовать процедуру шифрования, для четных (2,4,…,26) – дешифрования с использованием указанных методов. Ключ, используемый при шифровании, определите самостоятельно.

1-2. Исходную последовательность разбейте на группы по 4 символа. В каждой группе символы переставьте с использованием подстановки, выбираемой самостоятельно.

3-4. Исходную последовательность разбейте на группы по 4 символа. Реализуйте двойную перестановку каждой последовательности символов.

5-6. Исходную последовательность разбейте на группы по 8 символов. Реализуйте шифрование методом перестановки по заданному ключу, при этом четные группы символов шифровать в исходном направлении, нечетные – в обратном.

7-8. Исходную последовательность разбейте на группы по 8 символов. В каждой группе символы переставьте с использованием подстановки, выбираемой самостоятельно.

1. К правовым методам, обеспечивающим информационную безопасность, относятся:
   1.1. Разработка аппаратных средств обеспечения правовых данных

1.2. Разработка и установка во всех компьютерных правовых сетях журналов учета действий
1.3. Разработка и конкретизация правовых нормативных актов обеспечения безопасности (+)

2. Основными источниками угроз информационной безопасности являются все указанное в списке:
   2.1. Хищение жестких дисков, подключение к сети, инсайдерство
   2.2. Перехват данных, хищение данных, изменение архитектуры системы (+)
   2.3. Хищение данных, подкуп системных администраторов, нарушение регламента работы
3. Виды информационной безопасности:
   3.1. Персональная, корпоративная, государственная (+)
   3.2. Клиентская, серверная, сетевая
   3.3. Локальная, глобальная, смешанная
4. Цели информационной безопасности – своевременное обнаружение, предупреждение:
   4.1. несанкционированного доступа, воздействия в сети (+)
   4.2. инсайдерство в организации
   4.3. чрезвычайных ситуаций
5. Основные объекты информационной безопасности:
   5.1. Компьютерные сети, базы данных (+)
   5.2. Информационные системы, психологическое состояние пользователей
   5.3. Бизнес-ориентированные, коммерческие системы
6. Основными рисками информационной безопасности являются:
   6.1. Искажение, уменьшение объема, перекодировка информации
   6.2. Техническое вмешательство, выведение из строя оборудования сети
   6.3. Потеря, искажение, утечка информации (+)
7. К основным принципам обеспечения информационной безопасности относится:
   7.1. Экономической эффективности системы безопасности (+)
   7.2. Многоплатформенной реализации системы
   7.3. Усиления защищенности всех звеньев системы
8. Основными субъектами информационной безопасности являются:
   8.1. руководители, менеджеры, администраторы компаний
   8.2. органы права, государства, бизнеса (+)
   8.3. сетевые базы данных, фаерволлы
9. К основным функциям системы безопасности можно отнести все перечисленное:
   9.1. Установление регламента, аудит системы, выявление рисков (+)
   9.2. Установка новых офисных приложений, смена хостинг-компании
   9.3. Внедрение аутентификации, проверки контактных данных пользователей
10. Принципом информационной безопасности является принцип недопущения:
    10.1. Неоправданных ограничений при работе в сети (системе) (+)
    10.2. Рисков безопасности сети, системы
    10.3. Презумпции секретности

ОПК-3.3

Задание 1.

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 2.

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***

Варианты заданий

Для нечетных вариантов (1,3,…, 25) предлагается реализовать процедуру шифрования файлов, для четных (2,4,…, 26) – дешифрования с использованием указанных методов. Если ключ, используемый при шифровании, не указан, задайте его самостоятельно.

1-2. Зашифровать исходное сообщение с использованием системы шифрования Цезаря.

3-4. Зашифровать исходное сообщение, используя аффинную систему подстановок Цезаря при A=12, B=7.

5-6. Зашифровать исходное сообщение с использованием Полибианского квадрата. Заполнение таблицы размером 8x4 буквами алфавита реализовать в следующем порядке: сначала нечетные столбцы, затем – четные.

7-8. Зашифровать исходное сообщение с использованием лозунгового шифра. В качестве ключа использовать свое имя или фамилию.

1. К правовым методам, обеспечивающим информационную безопасность, относятся:
   1.1. Разработка аппаратных средств обеспечения правовых данных
   1.2. Разработка и установка во всех компьютерных правовых сетях журналов учета действий
   1.3. Разработка и конкретизация правовых нормативных актов обеспечения безопасности (+)
2. Основными источниками угроз информационной безопасности являются все указанное в списке:
   2.1. Хищение жестких дисков, подключение к сети, инсайдерство
   2.2. Перехват данных, хищение данных, изменение архитектуры системы (+)
   2.3. Хищение данных, подкуп системных администраторов, нарушение регламента работы
3. Виды информационной безопасности:
   3.1. Персональная, корпоративная, государственная (+)
   3.2. Клиентская, серверная, сетевая
   3.3. Локальная, глобальная, смешанная
4. Цели информационной безопасности – своевременное обнаружение, предупреждение:
   4.1. несанкционированного доступа, воздействия в сети (+)
   4.2. инсайдерство в организации
   4.3. чрезвычайных ситуаций
5. Основные объекты информационной безопасности:

5.1. Компьютерные сети, базы данных (+)
5.2. Информационные системы, психологическое состояние пользователей
5.3. Бизнес-ориентированные, коммерческие системы

6. Основными рисками информационной безопасности являются:
6.1. Искажение, уменьшение объема, перекодировка информации
6.2. Техническое вмешательство, выведение из строя оборудования сети
6.3. Потеря, искажение, утечка информации (+)

7. К основным принципам обеспечения информационной безопасности относится:
7.1. Экономической эффективности системы безопасности (+)
7.2. Многоплатформенной реализации системы
7.3. Усиления защищенности всех звеньев системы

8. Основными субъектами информационной безопасности являются:
8.1. руководители, менеджеры, администраторы компаний
8.2. органы права, государства, бизнеса (+)
8.3. сетевые базы данных, фаерволлы

9. К основным функциям системы безопасности можно отнести все перечисленное:
9.1. Установление регламента, аудит системы, выявление рисков (+)
9.2. Установка новых офисных приложений, смена хостинг-компании
9.3. Внедрение аутентификации, проверки контактных данных пользователей

10. Принципом информационной безопасности является принцип недопущения:
10.1. Неоправданных ограничений при работе в сети (системе) (+)
10.2. Рисков безопасности сети, системы
10.3. Презумпции секретности

3. Формы контроля

3.1. Формы текущего контроля

Текущий контроль по дисциплине проводится в виде тестовых опросов по отдельным темам дисциплины и проверки решений задач на практических занятиях,

3.2 Формы промежуточного контроля

Форма промежуточного контроля по дисциплине – проверка контрольных работ, выполняемых самостоятельно.

3.3. Формы заключительного контроля

Форма заключительного контроля по дисциплине – зачет.

4. Критерий допуска зачету

К зачету допускаются студенты, выполнившие ко дню проведения зачета по расписанию зачетной недели все контрольные работы.

Студенты, не выполнившие ко дню проведения зачета по расписанию хотя бы одну контрольную работу, на зачете получают оценку «не зачтено». Решение о повторном зачете и сроках проведения экзамена принимает деканат после ликвидации студентом имеющейся задолженности.

Составил
доцент кафедры ВПМ
к.т.н. Тишкина В.В.

Заведующий кафедрой ВПМ
д.т.н. Овечкин Г.В.