

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ  
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ  
УНИВЕРСИТЕТ»  
ВЫСШИЙ КОЛЛЕДЖ ПГТУ «ПОЛИТЕХНИК»

Зам. директора по УМР

Е.Ю. Кузнецов

«29» апреля 2022 г



**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ПРОФЕССИОНАЛЬНОМУ  
МОДУЛЮ  
ПМ.03 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ  
БЕЗОПАСНОСТИ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ  
И СЕТЯХ ВЕЩАНИЯ**

специальность 11.02.10 Радиосвязь, радиовещание и телевидение

РАССМОТРЕНО И ОДОБРЕНО

Предметно-цикловой комиссией

Протокол № 5

«28» апреля 2022 г.

Председатель ПЦК  /Е. Ю. Кузнецов /

Организация-разработчик: Высший колледж ПГТУ «Политехник»

Разработчик:

Савинов Александр Николаевич, к.т.н., доцент кафедры ФГБОУ ВО «ПГТУ».

## **СОДЕРЖАНИЕ**

### **1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ**

1.1. Область применения

1.2. Результаты освоения профессионального модуля, подлежащие проверке

### **2. ФОНД МАТЕРИАЛОВ ДЛЯ ОЦЕНКИ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

2.1. Оценочные средства для текущего контроля

2.2. Оценочные средства для итогового контроля (промежуточной аттестации)

# 1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

## 1.1. Область применения

Фонд оценочных средств (ФОС) предназначен для контроля и оценки результатов освоения профессионального модуля ПМ.03 Обеспечение информационной безопасности в телекоммуникационных системах и сетях вещания.

ФОС включает контрольно-оценочные материалы для проведения текущего контроля и промежуточной аттестации в форме дифференцированного зачета.

ФОС разработан в соответствии с:

- Положением о текущем контроле успеваемости и промежуточной аттестации обучающихся Поволжского государственного технологического университета СМК-ПМ-3.01-32-2021.
- Положением о рабочей программе учебной дисциплины, профессионального модуля и практики образовательной программы среднего профессионального образования в ФГБОУ ВО «ПГТУ» (СМК-ПИ-3.03-30-2021);
- ФГОС СПО (утвержден приказом Министерства образования и науки Российской Федерации №812 от 22.07.2014г., зарегистрирован Министерством юстиции России 25.08.2014 № 33770) по специальности 11.02.10 Радиосвязь, радиовещание и телевидение.
- Рабочей программой профессионального модуля ПМ.03 Обеспечение информационной безопасности в телекоммуникационных системах и сетях вещания по специальности СПО 11.02.10 Радиосвязь, радиовещание и телевидение.

## 1.2. Результаты освоения учебной дисциплины

В результате освоения профессионального модуля ПМ.03 Обеспечение информационной безопасности в телекоммуникационных системах и сетях вещания обучающийся должен обладать предусмотренными ФГОС СПО по специальности 11.02.10 Радиосвязь, радиовещание и телевидение и рабочей программой профессионального модуля ПМ.03 Обеспечение информационной безопасности в телекоммуникационных системах и сетях вещания следующими умениями, знаниями, которые формируют компетенции:

Код результата обучения	Результат обучения
1	2
<b>Общие и профессиональные компетенции</b>	
ОК 1	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.
ОК 2	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
ОК 3	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

<b>Код результата обучения</b>	<b>Результат обучения</b>
<i>1</i>	<i>2</i>
ОК 4	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
ОК 5	Использовать информационно-коммуникационные технологии в профессиональной деятельности.
ОК 6	Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.
ОК 7	Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.
ОК 8	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
ОК 9	Ориентироваться в условиях частой смены технологий в профессиональной деятельности.
ПК 3.1.	Использовать программно-аппаратные средства защиты информации в системах радиосвязи и вещания.
ПК 3.2.	Применять системы анализа защищенности для обнаружения уязвимостей в сетевой инфраструктуре, давать рекомендации по их устранению.
ПК 3.3.	Обеспечивать безопасное администрирование сетей вещания.

## 2. ФОНД МАТЕРИАЛОВ ДЛЯ ОЦЕНКИ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

### 2.1. Оценочные средства для текущего контроля

#### Типовая спецификация теста

#### 1 Назначение

Тест входит в состав комплекса оценочных средств и предназначается для текущего контроля и оценки знаний обучающихся по программе профессионального модуля ПМ.03 Обеспечение информационной безопасности в телекоммуникационных системах и сетях вещания программы подготовки специалистов среднего звена специальности 11.02.10 Радиосвязь, радиовещание и телевидение.

**2. Контингент обучающихся:** обучающиеся 4 курса специальности 11.02.10 Радиосвязь, радиовещание и телевидение

**3. Форма и условия контроля:** в письменном виде на бланках

**4. Время выполнения:** 45 мин.

подготовка – 2 мин.;

выполнение – 40 мин.

оформление и сдача – 3 мин.

**5. Соответствие тестовых вопросов** результатам освоения профессионального модуля, подлежащие проверке **(сформированности З,У, ПК, ОК)**

Результаты обучения (освоенные умения, усвоенные знания)	Коды формируемых профессиональных компетенций	№ тестового вопроса
<b>Уметь</b>		
классифицировать угрозы информационной безопасности	<i>ОК 1-9, ПК 3.1 – 3.3</i>	1-24
проводить выборку средств защиты в соответствии с выявленными угрозами		
определять возможные виды атак		
осуществлять мероприятия по проведению аттестационных работ		
разрабатывать политику безопасности объекта		
выполнять расчет и установку специализированного оборудования для максимальной защищенности объекта		
использовать программные продукты, выявляющие недостатки систем защиты		
производить установку и настройку средств защиты		
конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности		

выполнять тестирование систем с целью определения уровня защищенности		
использовать программные продукты для защиты баз данных		
применять криптографические методы защиты информации		
<b>Знать</b>		
каналы утечки информации	ОК 1-9, ПК 3.1 – 3.3	1-24
назначение, классификацию и принципы работы специализированного оборудования		
принципы построения информационно-коммуникационных сетей		
возможные способы несанкционированного доступа		
законодательные и нормативные правовые акты в области информационной безопасности		
правила проведения возможных проверок		
этапы определения конфиденциальности документов объекта защиты		
структуру систем условного доступа и принцип их работы		
возможные способы, места установки и настройки программных продуктов		
конфигурации защищаемых сетей		
алгоритмы работы тестовых программ		
собственные средства защиты различных операционных систем и сред		
способы и методы шифрования информации		

## 6. Структура теста

Инструкция: Выберите **один** правильный вариант и запишите его букву.

**1. Полоса эффективно передаваемых частот стандартного канала тональной частоты находится в пределах:**

- а) от 200 Гц до 20 МГц
- б) от 300 Гц до 3,4 кГц
- в) от 15 Гц до 15кГц

**2. Телефонная нагрузка - это ...**

- а. суммарное время занятия соединительных путей коммутационной системы за определенный промежуток времени
- б) общее время разговора
- в) масса груза, положенного на телефон

**3. Часть поступающей телефонной нагрузки, не обслуженная из-за отсутствия свободных соединительных путей в коммутационной системе, называется**

- а) обслуженной телефонной нагрузкой
- б) потерянной телефонной нагрузкой
- в) поступающей телефонной нагрузкой

**4. Суммарное время занятия всех соединительных путей коммутационной системы за определенный промежуток времени называется**

- а) обслуженной телефонной нагрузкой
- б) потерянной телефонной нагрузкой
- в) поступающей телефонной нагрузкой

**5. Нагрузка, которая была бы обслужена, если бы каждому поступившему вызову был тотчас предоставлен один из соединительных путей коммутационной системы и соединение доведено до конца, называется**

- а) обслуженной телефонной нагрузкой
- б) потерянной телефонной нагрузкой
- в) поступающей телефонной нагрузкой

**6. Перечислите уровни архитектуры взаимодействия открытых систем в порядке от общего к детальному:**

- A. Канальный уровень
- B. Сеансовый уровень
- C. Физический уровень
- D. Сетевой уровень
- E. Прикладной уровень
- F. Транспортный уровень
- G. Уровень представления

**7. Режим переноса информации, основанной на пакетной коммутации с минимумом функций, выполняемых узлами коммутации на уровне звена с целью повышения уровня прозрачности сети называется**

- а) синхронный режим доставки (STM)
- б) асинхронный режим доставки (ATM)
- в) быстрая коммутация пакетов

**8. Рабочее затухание канала при конечных нагрузках 600 Ом называется**

- а) остаточным затуханием канала
- б) промежуточным затуханием канала
- в) систематическим затуханием канала

**9. Зависимость остаточного затухания канала от частоты при постоянном уровне на входе канала называется**

- а) амплитудной характеристикой канала
- б) фазовой характеристикой канала
- в) частотной характеристикой канала



**10. Зависимость фазовой постоянной канала от частоты называется**

- а) временной характеристикой канала
- б) фазовой характеристикой канала
- в) частотной характеристикой канала

**11. Зависимость остаточного затухания от уровня на входе, измеренная при неизменной частоте измерительного генератора называется**

- а) временной характеристикой канала
- б) фазовой характеристикой канала
- в) частотной характеристикой канала

**12. Посторонние токи, частотный спектр которых совпадает со спектром передаваемых сигналов, называются**

- а) сигналами
- б) помехами
- в) постоянными составляющими

**13. Устройство АРУ - это**

- а) устройство асинхронного ручного управления
- б) устройство апериодического разделяющего усилителя
- в) устройство с автоматической регулировкой уровня

**14. Существующие типы систем цифровой иерархии - это**

- а) плезиохронная и синхронная
- б) цифровая и дискретная
- в) асинхронная и аналоговая

**15. Вид ЦСП, при котором информация передается по оптическим волокнам, объединенным в волоконно-оптический кабель, называется**

- а) волоконно-оптической цифровой системой передачи
- б) оптической системой передачи
- в) кабельной системой передачи

**16. Сети односторонней мобильной связи, обеспечивающие передачу коротких сообщений из центра системы на миниатюрные абонентские приемники называются**

- а) пейджинговыми сетями
- б) транкинговыми сетями
- в) мобильными сетями

**17. Устройство, добавляющее в цифровой сигнал, получаемый с выхода кодера речи, дополнительную информацию, предназначенную для защиты от ошибок за счет введения избыточности при передаче сигнала по линии связи называется**

- а) антенным блоком
- б) логическим блоком
- в) кодером канала

**18. Устройство, преобразующее принятый цифровой сигнал речи в аналоговую форму и подающее его на вход динамика называется**

- а) АЦП
- б) ЦАП
- в) Синтезатором

**19. Источник колебания несущей частоты, используемой для передачи информации по радиоканалу называется**

- а) АЦП
- б) ЦАП
- в) Синтезатором

**20. Устройство, преобразующее в цифровую форму сигнал с выхода микрофона, и осуществляющее последующую обработку и передачу сигнала речи в цифровой форме называется**

- а) АЦП
- б) ЦАП
- в) Синтезатором

**21. Автоматическая телефонная станция сети сотовой связи, обеспечивающая все функции управления сетью называется**

- а) автоматическим обработчиком
- б) устройством управления сигналами
- в) центром коммутации

**22. Несколько спутников-ретрансляторов, равномерно распределенных на определенных орбитах, и образующих космическую группировку, называются**

- а) космическим сегментом
- б) ретранслирующей связкой
- в) орбитальной станцией

**23. При осуществлении связи по спутниковому телефону требуется ориентация на спутник?**

- а) да
- б) нет

**24. Часть территории, которую необходимо охватить вещанием при заданном уровне сигнала называют**

- а) зоной обслуживания
- б) поверхностью земли
- в) вещательной территорией

#### **КРИТЕРИИ ОЦЕНКИ**

Оценка	Баллы, %	Количество правильных ответов
5	100-90	23-24
4	89-70	18-22
3	69-50	13-17
2	49 и менее	12 и менее

## **2.2.Оценочные средства для итогового контроля (промежуточной аттестации)**

### **2.2.1 Перечень вопросов к дифференцированному зачету**

#### **МДК.03.01 Технология применения комплексной системы защиты информации в системах радиосвязи и радиовещания**

- 1 Понятие информационной безопасности, характеристика ее составляющих. Место информационной безопасности в системе национальной безопасности.
- 2 Концептуальная модель защиты информации. Проблемы информационной безопасности в сфере телекоммуникаций: объекты защиты; виды защиты; системы защиты информации.
- 3 Классификация и анализ угроз информационной безопасности в телекоммуникационных системах. Виды уязвимости информации и формы ее проявления.
- 4 Понятие о конфиденциальной информации (грифы, закон о государственной тайне, закон о личной тайне, закон о коммерческой тайне).
- 5 Уровни информационной безопасности – законодательно-правовой, административно-организационный, программно-технический. Принципы построения систем защиты информации.
- 6 Информация как объект права. Нормативно-правовые основы информационной безопасности в РФ.
- 7 Законодательно - нормативные акты в области обеспечения информационной безопасности, защиты государственной тайны и конфиденциальной информации.
- 8 Конституционные гарантии прав граждан в области информационной безопасности. Понятие и виды защищаемой информации по законодательству РФ.
- 9 Система защиты государственной тайны, правовой режим защиты государственной тайны.
- 10 Лицензирование и сертификация в области защиты информации. Стандартизация информационной безопасности.
- 11 Сущность и сферы действия организационной защиты информации.
- 12 Механизмы обеспечения информационной безопасности. Разработка политики безопасности.
- 13 Проведение анализа угроз и расчета рисков в области информационной безопасности.
- 14 Выбор механизмов и средств обеспечения информационной безопасности. Модели защиты информационных систем.
- 15 Правила организации работ подразделений защиты информации. Разработка инструкций по работе со средствами защиты.
- 16 Организация работы персонала с конфиденциальной информацией.

### **МДК.03.02 Технология использования систем условного доступа в сетях вещания**

- 1 Информационная безопасность в телекоммуникационных и информационно-коммуникационных сетях.
- 2 Структурные схемы систем защиты информации в типовых информационных системах. Показатели защищенности телекоммуникационных систем.
- 3 Сервисы, обеспечивающие информационную безопасность в многоканальных телекоммуникационных системах и сетях электросвязи: ограничение физического доступа к автоматизированным системам; идентификация и аутентификация пользователей; ограничение доступа в систему; разграничение доступа; регистрация событий (аудит).
- 4 Криптографическая защита; контроль целостности; управление политиками безопасности; уничтожение остаточной информации; резервирование данных; сетевая защита; защита от утечки и перехвата информации по техническим каналам. Подсистемы безопасности.
- 5 Типовые удаленные сетевые атаки и их характеристика. Компьютерные вирусы и защита от них. Антивирусные программы и комплексы.
- 6 Построение систем антивирусной защиты телекоммуникационных систем и сетей.
  - 1 Технологии защиты данных. Принципы криптографической защиты информации (симметричные и асимметричные алгоритмы шифрования, электронная цифровая подпись, стеганография).
  - 2 Различные технологии аутентификации. Технологии защиты межсетевого обмена данных. Технология обеспечения безопасности сетевых операционных систем. Основы технологии виртуальных защищенных сетей VPN.

- 3    Технология обнаружения вторжений (анализ защищенности и обнаружения сетевых атак). Требования по защите от несанкционированного доступа Технические средства обеспечения безопасности многоканальных телекоммуникационных систем.
- 4    Многоуровневая защита корпоративных сетей. Режим функционирования межсетевых экранов и их основные компоненты. Маршрутизаторы. Шлюзы сетевого уровня. Усиленная аутентификация. Основные схемы сетевой защиты на базе межсетевых экранов. Применение межсетевых экранов для организации виртуальных корпоративных сетей. Программные методы защиты информации. Защита компьютерных систем от удаленных атак через сеть Internet.
- 5    Классификация способов защиты информации в компьютерных сетях. Понятие разрушающего программного воздействия. Модели взаимодействия прикладной программы и программной закладки. Методы перехвата и навязывания информации. Методы внедрения программных закладок.
- 6    Компьютерные вирусы как особый класс разрушающих программных воздействия. Защита от разрушающих программных воздействий. Антивирусная защита в сетях. Понятие изолированной программной среды. Рекомендации по защите информации Internet.
- 7    Организационные требования к системам информационной защиты ИС. Требования по обеспечению информационной безопасности к аппаратным средствам и программному обеспечению. Требования по применению способов, методов и средств защиты информации. Требования к документированию событий в системе и выявлению несанкционированного доступа. Организация аудита информационной безопасности ИС и предприятия в целом.

### **Критерии оценки ответа**

«Отлично» - теоретическое содержание курса освоено полностью, без пробелов, умения сформированы, все предусмотренные программой учебные задания выполнены, качество их выполнения оценено высоко.

«Хорошо» - теоретическое содержание курса освоено полностью, без пробелов, некоторые умения сформированы недостаточно, все предусмотренные программой учебные задания выполнены, некоторые виды заданий выполнены с ошибками.

«Удовлетворительно» - теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые умения работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий содержат ошибки.

«Неудовлетворительно» - теоретическое содержание курса не освоено, необходимые умения не сформированы, выполненные учебные задания содержат грубые ошибки.