

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Выборнова Любовь Алексеевна
Должность: Ректор
Дата подписания: 21.08.2024 13:55:42
Уникальный программный ключ:
c3b3b9c625f6c113afa2a2c42baff9e05a38b76e

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Товолжский государственный университет сервиса» (ФГБОУ ВО «ПВГУС»)

УТВЕРЖДЕНО

на заседании

Высшей школы передовых

производственных технологий

Протокол от 30.08.2024 № 1

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
(фонд оценочных средств) для проведения промежуточной аттестации
по дисциплине

«Защита информации в инфокоммуникациях»

наименование дисциплины

по образовательной программе высшего образования – программе

бакалавриата

бакалавриата, специалитета,

магистратуры

«Информационные технологии в инфокоммуникациях»

наименование образовательной программы

11.03.02 «Инфокоммуникационные технологии и системы связи»

шифр, наименование направления подготовки / специальности

Составитель

ст.преподаватель, ВШППТ, Васильева А.С.

ФИО, должность, структурное подразделение,
ученая степень, ученое звание

Тольятти
2024

1. Паспорт фонда оценочных средств (далее – ФОС)

1.1. Планируемые результаты обучения по дисциплине

Код компетенции	Наименование компетенции	Код и наименование индикаторов достижения компетенции
ОПК-3	Способен применять методы поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационной безопасности	ИОПК-3.1. Применяет в профессиональной деятельности знания основных закономерностей передачи информации в инфокоммуникационных системах, основных видов сигналов, используемых в телекоммуникационных системах, особенностей передачи различных сигналов по каналам и трактам телекоммуникационных систем ИОПК-3.2. Применяет в профессиональной деятельности знания принципов, основных алгоритмов и устройств цифровой обработки сигналов; принципов построения телекоммуникационных систем различных типов и способов распределения информации в сетях связи ИОПК-3.3. Решает задачи обработки данных с помощью средств вычислительной техники ИОПК-3.4. Применяет в профессиональной деятельности методы обеспечения информационной безопасности

В результате изучения дисциплины обучающийся должен:

Знать: Основные понятия и терминологию в области защиты информации в инфокоммуникационных системах

Нормативно-правовую базу в сфере информационной безопасности и защиты персональных данных

Принципы построения защищённых инфокоммуникационных систем и сетей

Методы и средства криптографической защиты информации

Виды угроз безопасности информации в инфокоммуникационных системах

Уметь: Анализировать угрозы безопасности информации в инфокоммуникационных системах

Разрабатывать политики безопасности для инфокоммуникационных систем

Применять криптографические методы защиты информации

Осуществлять настройку и конфигурирование средств защиты информации

Владеть: Навыками анализа защищённости инфокоммуникационных систем

Методами обеспечения конфиденциальности, целостности и доступности информации

Технологиями криптографической защиты данных

Практическими навыками настройки и администрирования систем защиты информации

1.2. Содержание дисциплины

№	Тема (раздел дисциплины) (в соответствии с РПД)	Код компетенции
1	Тема 1. Введение в информационную безопасность.	ОПК-3
2	Тема 2. Правовое обеспечение информационной безопасности.	ОПК-3
3	Тема 3. Организационное обеспечение информационной безопасности.	ОПК-3
4	Тема 4. Технические средства и методы защиты информации.	ОПК-3
5	Тема 5. Программно-аппаратные средства и методы обеспечения информационной безопасности.	ОПК-3
6	Тема 6. Криптографические методы защиты информации.	ОПК-3

1.3. Система оценивания по дисциплине

Дисциплина изучается в течение одного семестра
Форма промежуточной аттестации по дисциплине – зачет.

Шкалы оценки уровня сформированности результатов обучения		Шкала оценки уровня освоения дисциплины		
Уровневая шкала оценки компетенций	100 балльная шкала, %	100 балльная шкала, %	5-балльная шкала, дифференцированная оценка/балл	недифференцированная оценка
допороговый	ниже 61	ниже 61	«неудовлетворительно» / 2	не зачтено
пороговый	61-85,9	61-69,9	«удовлетворительно» / 3	зачтено
		70-85,9	«хорошо» / 4	зачтено
повышенный	86-100	86-100	«отлично» / 5	зачтено

2. Перечень оценочных материалов для проведения промежуточной аттестации

Вопросы для подготовки к зачету

	Содержание вопроса
ОПК-3. Способен применять методы поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационной безопасности	
1.	Информационная безопасность — это: а) Конфиденциальность информации б) Защищённость информации и инфраструктуры от воздействий, наносящих ущерб в) Доступность информации г) Гибкость информационных систем
2.	Какие уровни защиты информации существуют: а) Индустриальный б) Административный в) Законодательный г) Промышленный
3.	Криптография занимается: а) Исследованием конечных множеств знаков б) Поиск и исследованием математических методов преобразования информации в) Упорядочиванием наборов из элементов алфавита г) Преобразованием открытого текста в зашифрованный
4.	Электронная цифровая подпись — это: а) Документ в электронно-цифровой форме б) Реквизит электронного документа для защиты от подделки в) Документ на бумажном носителе г) Средство аутентификации участников информационного взаимодействия
5.	Шифры бывают: а) Симметричные б) Асимметричные в) Блочные г) Поточные
6.	Угроза безопасности информации — это: а) Потенциальная возможность нарушить информационную безопасность б) Система программных средств в) Процесс определения требований г) Технические средства защиты
7.	Защита информации — это: а) Процесс сбора и обработки информации б) Преобразование информации для непонятности в) Деятельность по предотвращению утечки информации г) Совокупность правил доступа к информации
8.	К основным методам защиты информации относятся: а) Правовые б) Технические в) Организационные г) Экономические
9.	Какой стандарт шифрования считается наиболее надёжным для Wi-Fi сетей? а) WEP б) WPA в) WPA2 г) WPA3
10.	Что такое атака «человек посередине» (Man-in-the-Middle)? а) Атака на сетевое оборудование б) Внедрение в существующее подключение для перехвата данных

	Содержание вопроса
	c) DDoS-атака d) Создание ложной точки доступа
11.	Какая технология используется для передачи данных на расстояние до 20 см? a) Bluetooth b) NFC c) Wi-Fi d) GPRS
12.	Что такое SSID в контексте беспроводных сетей? a) Пароль для доступа к сети b) Тип шифрования c) Имя беспроводной сети d) MAC-адрес точки доступа
13.	Какой протокол обеспечивает безопасную передачу данных в беспроводных сетях? a) HTTP b) FTP c) HTTPS d) SMTP
14.	Какой метод аутентификации считается наиболее надёжным? a) Открытая аутентификация b) Аутентификация по паролю c) Аутентификация по сертификатам d) Одноразовые пароли
15.	Что такое WPS (Wi-Fi Protected Setup)? a) Протокол шифрования b) Метод аутентификации c) Упрощённая настройка безопасности d) Тип беспроводной сети
16.	Как называется атака, при которой злоумышленник перехватывает данные между двумя устройствами?
17.	Как называется процесс проверки подлинности устройства в сети?
18.	Что такое WPS?
19.	Какой метод защиты рекомендуется для публичных Wi-Fi сетей?
20.	Как называется процесс проверки целостности данных?
21.	Что такое EAP?
22.	Какой тип беспроводной сети используется для покрытия города?
23.	Основной закон РФ в сфере информационной безопасности?
24.	Три основных принципа защиты информации?
25.	Средство защиты от вредоносных программ?
26.	Наука о методах обеспечения информационной безопасности?
27.	Метод защиты, основанный на разграничении доступа?
28.	Метод защиты, основанный на маскировке информации?
29.	Процесс выявления угроз безопасности?
30.	Процесс оценки уровня безопасности?