

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Выборнова Любовь Алексеевна
Должность: Ректор
Дата подписания: 21.08.2026 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 кафедры
«Информационный и электронный
сервис»

Протокол от 28.05.2021 № 10

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

«Защита информации»

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 Яницкая Т.С. к.т.н

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

Тольятти
2021

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: методы защиты информации

Уметь: соблюдать основные требования информационной безопасности

Владеть: навыками применения методов 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	ОПК-3:

	ИНФОРМАЦИИ	
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

Форма проведения промежуточной аттестации по дисциплине зачет

Устно-письменная форма по экзаменационным билетам предполагается, как правило, для сдачи академической задолженности.

Примерный перечень вопросов и заданий для подготовки к зачету

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. Кто в РФ осуществляет общее руководство системой информационной безопасности
2. В каком году был принят закон РФ «Об информации, информационных технологиях и о защите информации»
3. Аутентификация субъекта — это
4. Как классифицируются угрозы безопасности информационным системам
5. Политика безопасности - это
6. Алгоритмы криптографического преобразования информации - это
7. Доступ к информации различают
8. Санкционированный доступ к информации — это
9. Несанкционированный доступ к информации характеризуется

10. Угрозы безопасности ИС по природе возникновения бывают

Примерный тест для итогового тестирования:

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. Raid-массив это:

Набор жестких дисков, подключенных особым образом

Антивирусная программа

Вид хакерской утилиты

2. Выберите составные части современного антивируса

Модем

Сканер

Межсетевой экран

Принтер

3. К вредоносным программам относятся:

Потенциально опасные программы

Вирусы, черви, трояны

Межсетевой экран, брандмауэр

4. К биометрической системе защиты относятся

Защита паролем

Физическая защита данных

Идентификация по отпечатку пальца

5. Вредоносная программа, которая подменяет собой загрузку некоторых программ при загрузке системы называется

Загрузочный вирус

Макровирус

Троян

Сетевой червь

Файловый вирус

6. Вредоносная программа - это...

любое ПО, предназначенное для получения несанкционированного доступа к информации, которая хранится на компьютере, с целью причинения вреда владельцу компьютера.

любое ПО, предназначенное для получения санкционированного доступа к информации, которая хранится на компьютере, с целью причинения вреда владельцу компьютера.

любое ПО, предназначенное для обеспечения контроля над компьютером злоумышленника.

любое ПО, предназначенное для обеспечения контроля над компьютерами учащихся.

7. Шпионские программы - это...

ПО, которое тайно устанавливается и используется для доступа к информации, хранимой на компьютере.

ПО, которое открыто устанавливается и используется для доступа к информации, хранимой на компьютере.

ПО, которое предназначено для удаления информации с компьютера.

ПО, которое предназначено для удалённого управления и сортировки информации на компьютере.

8. Антивирусная программа - это...

программа, предназначенная для обнаружения и удаления компьютерных вирусов, а также для эффективной защиты от них.

программа, предназначенная для сокрытия компьютерных вирусов.

программа, предназначенная для обнаружения вирусов и извещения о них правоохранительных органов.

программа, которая используется правоохранительными органами для выявления несанкционированного доступа к образовательным ресурсам.

9. Файловые вирусы - это...

вредоносные программы, работа которых заключается в распространении своих копий по всему компьютеру.

вредоносные программы, которые заражают загрузочный сектор гибкого или жёсткого диска.

заражают файлы *.exe, *.sys, *.dll

вирусы, которые поражают файлы приложений Microsoft Office.

10. Загрузочные вирусы - это...

вредоносные программы, которые заражают загрузочный сектор гибкого или жёсткого диска.

вредоносные программы, работа которых заключается в распространении своих копий по всему компьютеру.

вредоносные программы, которые тайно устанавливаются и используются для доступа к информации, хранимой на компьютере.

вредоносные программы, которые распространяются через электронную почту и сеть Интернет.

11. Сетевые вирусы - это...

вирусы, которые распространяются по компьютерной сети.

вредоносные программы, которые осуществляют тайные действия по сбору, изменению и передаче информации злоумышленникам.

вредоносные программы, с помощью которых можно выполнять скрытое удалённое управление компьютером.

программное обеспечение, которое может нанести косвенный вред компьютеру, на котором установлено, или другим компьютерам в сети.

12. Макровирусы - это...

вирусы, которые поражают файлы приложений Microsoft Office.

вирусы, которые заражают загрузочный сектор гибкого или жёсткого диска.

вирусы, которые тайно устанавливаются и используются для доступа к информации, хранимой на компьютере.

вирусы, которые распространяются через электронную почту и сеть Интернет.

13. Какие существуют типы вредоносных программ?

Вирусы, черви, троянские и хакерские программы.

Шпионские и рекламные программы.

Потенциально опасное программное обеспечение.

Трояны-шпионы.

Сигнатуры.

Макросы

14. Какие действия может выполнять антивирусная программа с обнаруженным заражённым файлом?

Только отчёт.

Лечить.

Удалить.

Переименовать.

Пропустить.

Карантин.

Создать копию.

Удалить только расширение.

15. Выберите верные утверждения, которыми нужно пользоваться при задании пароля.

Пароль не должен легко раскрываться.

Подбор пароля должен быть максимально сложным.

В основе пароля не должно находиться ваше имя, кличка животного, дата рождения и т. д.

Не стоит записывать пароль.

Для большей надёжности нужно записать пароль куда-либо и положить рядом с компьютером.

В основе пароля должно находиться ваше имя, кличка животного, дата рождения и т. д.

Полный фон оценочных средств для проведения промежуточной аттестации размещен в банке вопросов электронного учебного курса дисциплины в ЭИОС университета <http://sdo.tolgas.ru/>, а также хранится в бумажном и (или) электронном виде на кафедре-разработчике.