

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Выборнова Любовь Алексеевна  
Должность: Ректор  
Дата подписания: 12.10.2026 12:54:32  
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 Ученого совета

Высшей школы интеллектуальных  
систем и кибертехнологий

Протокол от 23.05.2025 № 10

### ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

(фонд оценочных средств) для проведения промежуточной аттестации  
по дисциплине

«Основы управления информационной безопасностью»

наименование дисциплины

по образовательной программе высшего образования – программе

бакалавриата

бакалавриата, специалитета,  
магистратуры

«Организация и технологии защиты информации (по отрасли или в сфере  
профессиональной деятельности)»

наименование образовательной программы

10.03.01 «Информационная безопасность»

шифр, наименование направления подготовки / специальности

Составитель

Мунирова Ю.С.,  
старший преподаватель Высшей школы  
интеллектуальных систем и кибертехнологий  
Курцев Е.А., ассистент Высшей школы  
интеллектуальных систем и кибертехнологий

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

Тольятти  
2025

## 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-10          | Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты                                  | ИОПК-10.1. Разрабатывает Политику информационной безопасности, включая цели, задачи, принципы обеспечения информационной безопасности, ответственность за нарушение Политики<br>ИОПК-10.2. Организует и поддерживает выполнение работы по применению мер обеспечения информационной безопасности<br>ИОПК-10.3. Осуществляет управление процессом обеспечения информационной безопасности |
| ОПК-6.          | Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю | ИОПК-6.1. Применяет технологии, методы и средства защиты информации ограниченного доступа<br>ИОПК-6.2. Знает и применяет положения действующих в РФ нормативных правовых актов, нормативных и методических документов по вопросам организации защиты информации ограниченного доступа                                                                                                    |

В результате изучения дисциплины обучающийся должен:

#### **Знает:**

- принципы и функции управления информационной безопасностью; структуру и порядок разработки политики информационной безопасности организации
- основы построения и функционирования системы менеджмента информационной безопасности, методы оценки и управления рисками
- технологии, методы и средства защиты информации ограниченного доступа
- нормативные правовые акты, нормативные и методические документы ФСТЭК России и ФСБ России по вопросам организации защиты информации ограниченного доступа

#### **Умеет:**

- разрабатывать отдельные разделы политики информационной безопасности организации
- организовывать выполнение комплекса мер по обеспечению информационной безопасности и управлять процессом их реализации на объекте защиты
- организовывать защиту информации ограниченного доступа с учетом требований регуляторов
- применять нормативные и методические документы при решении задач управления информационной безопасностью

#### **Владеет:**

- навыками управления процессом обеспечения информационной безопасности, включая планирование, контроль и совершенствование системы защиты
- навыками организации защиты информации ограниченного доступа в соответствии с действующими нормативными правовыми актами

## 1.2. Содержание дисциплины

| № | Тема (раздел дисциплины)<br>(в соответствии с РПД)                                     | Код компетенции |
|---|----------------------------------------------------------------------------------------|-----------------|
|   | Тема 1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК ОБЪЕКТ УПРАВЛЕНИЯ                              | ОПК-10          |
|   | ТЕМА 2. ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ                               | ОПК-10          |
|   | ТЕМА 3. СИСТЕМА МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ                                | ОПК-10          |
|   | ТЕМА 4. ОЦЕНКА И УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ                        | ОПК-6           |
|   | ТЕМА 5. ОРГАНИЗАЦИЯ ЗАЩИТЫ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА                            | ОПК-6           |
|   | ТЕМА 6. НОРМАТИВНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ    | ОПК-6           |
|   | ТЕМА 7. УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ                             | ОПК-10          |
|   | ТЕМА 8. КОНТРОЛЬ И АУДИТ ЭФФЕКТИВНОСТИ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ | ОПК-10<br>ОПК-6 |

## 1.3. Система оценивания по дисциплине

Дисциплина изучается в течение одного семестра

Форма промежуточной аттестации - экзамен.

| Шкала оценки уровня сформированности компетенций |                       | Шкала оценки уровня освоения дисциплины |                             |
|--------------------------------------------------|-----------------------|-----------------------------------------|-----------------------------|
| Уровневая шкала оценки компетенций               | 100 балльная шкала, % | 100 балльная шкала, %                   | недифференцированная оценка |
| Допороговый                                      | ниже 61               | ниже 61                                 | не зачтено                  |
| Пороговый                                        | 61-85,9               | 61-69,9                                 | зачтено                     |
|                                                  |                       | 70-85,9                                 | зачтено                     |
| Повышенный                                       | 86-100                | 86-100                                  | зачтено                     |

## 2. Перечень оценочных материалов для проведения промежуточной аттестации

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в ходе текущего контроля успеваемости (в процессе проведения практических занятий, тестирования, опросов).

В ходе проведения зачета осуществляется итоговый контроль и оценка результатов освоения компетенций.

### Вопросы для подготовки к экзамену

**ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты**

1. Понятие, цели и задачи управления информационной безопасностью организации.
2. Субъекты и объекты управления информационной безопасностью.
3. Принципы и функции управления информационной безопасностью.
4. Понятие и назначение политики информационной безопасности организации.
5. Структура и порядок разработки политики информационной безопасности.
6. Ответственность за нарушение положений политики информационной безопасности.
7. Понятие системы менеджмента информационной безопасности (СМИБ).
8. Цикл Деминга (PDCA) в управлении информационной безопасностью.
9. Стандарты серии ГОСТ Р ИСО/МЭК 27001 и их применение при построении СМИБ.
10. Понятие риска информационной безопасности, его составляющие.
11. Методы идентификации и оценки рисков информационной безопасности.
12. Способы обработки рисков информационной безопасности.
13. Понятие инцидента информационной безопасности, его классификация.
14. Процесс управления инцидентами информационной безопасности.
15. Порядок информирования о компьютерных инцидентах, взаимодействие с ГосСОПКА.
16. Понятие и виды контроля (аудита) информационной безопасности.
17. Показатели и критерии оценки эффективности системы управления информационной безопасностью.
18. Порядок проведения внутреннего аудита информационной безопасности организации.

**ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю**

1. Понятие и виды информации ограниченного доступа.
2. Правовой режим государственной тайны.
3. Правовой режим конфиденциальной информации и персональных данных.
4. Технологии, методы и средства защиты информации ограниченного доступа.
5. Порядок допуска и доступа персонала к информации ограниченного доступа.
6. Разработка перечня сведений конфиденциального характера организации.
7. Система нормативных правовых актов, регламентирующих управление информационной безопасностью в РФ.
8. Методические документы ФСТЭК России в области защиты информации ограниченного доступа.

9. Методические документы ФСБ России в области защиты информации ограниченного доступа.
10. Локальные нормативные акты организации в области информационной безопасности.
11. Лицензирование деятельности в области защиты информации.
12. Сертификация средств защиты информации.
13. Категорирование информации и объектов информатизации.
14. Организация защиты информации ограниченного доступа при взаимодействии с контрагентами.
15. Ответственность за нарушение требований по защите информации ограниченного доступа.