Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Выборнова Любовь Алексеевна
Должность: Ректор
Дата подписания: 30.10.2026 13:32:54
Уникальный программный ключ:
c3b3b9c625f6c113afa2a2c42baff9e05a38b76e

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

УТВЕРЖДЕНО

на заседании Ученого совета Высшей школы интеллектуальных систем и кибертехнологий

Протокол от 23.05.2025 г. № 10

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

Б.1.О.03.15 «Организационное и правовое обеспечение информационной безопасности»
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 Ю.С. Мунирова.,
старший преподаватель Высшей школы интеллектуальных систем и кибертехнологий
ФИО, должность, структурное подразделение, ученая степень, ученое звание

Тольятти
2023

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-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	ИОПК-5.1. Использует нормативные правовые документы в своей профессиональной деятельности ИОПК-5.2. Осуществляет подбор, изучение и обобщение научно- технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности
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 ИОПК-10.2. Организует и поддерживает выполнение работы по применению мер обеспечения информационной безопасности ИОПК-10.3. Осуществляет управление процессом обеспечения информационной безопасности

В результате изучения дисциплины обучающийся должен:

Знать: структуру законодательства РФ в области информационной безопасности; правовые режимы информации ограниченного доступа; полномочия регуляторов в области защиты информации; виды ответственности за правонарушения в информационной сфере; структуру и содержание политики информационной безопасности, частных политик и регламентов; задачи и функции службы защиты информации;

Уметь: определять применимые нормативные правовые акты и методические документы для конкретной ситуации; квалифицировать сведения по видам тайны; анализировать правоприменительную практику; разрабатывать проекты положений, инструкций, приказов по защите информации; организовывать допуск персонала к информации ограниченного доступа; планировать мероприятия по защите информации

Владеть: навыками поиска и анализа нормативных документов в справочно-правовых системах; навыками подготовки правовых обоснований решений по защите информации; навыками контроля соблюдения требований политики информационной безопасности и режима конфиденциальности; навыками документирования и разбора инцидентов информационной безопасности

1.2. Содержание дисциплины

№	Тема (раздел дисциплины) (в соответствии с РПД)	Код компетенции
1	Тема 1. Информационная безопасность как объект организационного и правового регулирования	ОПК-5 ОПК-10
2	Тема 2. Система законодательства Российской Федерации в области информационной безопасности	
3	Тема 3. Правовые режимы информации ограниченного доступа	
4	Тема 4. Правовое регулирование обработки и защиты персональных данных	
5	Тема 5. Государственная система защиты информации. Лицензирование и сертификация	
6	Тема 6. Политика информационной безопасности и организационно-распорядительная документация	
7	Тема 7. Организационные меры защиты информации. Служба защиты информации	
8	Тема 8. Ответственность за правонарушения в информационной сфере. Реагирование на инциденты	

1.3. Система оценивания по дисциплине

Дисциплина изучается в течение одного семестра
Форма промежуточной аттестации - зачет.

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.

Перечень вопросов к зачету

ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности

1. Понятия информации, информационной безопасности и защиты информации.
2. Доктрина информационной безопасности РФ: национальные интересы и угрозы.
3. Соотношение правовых, организационных и технических мер защиты информации.
4. Структура законодательства РФ в области информационной безопасности.
5. Федеральный закон № 149-ФЗ: основные понятия и принципы.
6. Классификация информации по категориям доступа.
7. Перечень сведений конфиденциального характера (Указ Президента РФ № 188).
8. Государственная тайна: понятие, степени секретности, грифы.
9. Допуск и доступ к государственной тайне.
10. Коммерческая тайна: понятие и режим коммерческой тайны.
11. Охрана конфиденциальности информации в рамках трудовых и гражданско-правовых отношений.
12. Служебная информация ограниченного распространения.
13. Профессиональные тайны: виды и правовое регулирование.
14. Федеральный закон № 152-ФЗ: принципы и условия обработки персональных данных.
15. Права субъекта персональных данных и обязанности оператора.
16. Уровни защищенности персональных данных и требования к их обеспечению.
17. Состав мер по обеспечению безопасности персональных данных (Приказ ФСТЭК России № 21).

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

18. Государственная система защиты информации: органы и их полномочия.
19. Лицензирование деятельности в области защиты информации.
20. Сертификация средств защиты информации и аттестация объектов информатизации.
21. Правовое регулирование безопасности КИИ (Федеральный закон № 187-ФЗ).
22. Политика информационной безопасности: структура и порядок разработки.
23. Организационно-распорядительная документация по защите информации.
24. Требования ГОСТ Р ИСО/МЭК 27001 к СМИБ.
25. Работа с персоналом в целях защиты информации.
26. Пропускной и внутриобъектовый режим.
27. Служба защиты информации: задачи, функции, структура.
28. Виды юридической ответственности за правонарушения в информационной сфере.
29. Преступления в сфере компьютерной информации (гл. 28 УК РФ).
30. Административная ответственность в области связи и информации.
31. Служебное расследование по факту нарушения режима конфиденциальности.
32. Управление инцидентами информационной безопасности.