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 № 10

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

Б1.В.ДВ.05.2 «Управление рисками информатизации бизнеса»
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
Ростова Е.П.,
старший преподаватель 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-10.2. Организует и поддерживает выполнение работы по применению мер обеспечения информационной безопасности ИОПК-10.3. Осуществляет управление процессом обеспечения информационной безопасности
ПК-7.	Способен организовать, поддерживать и управлять процессом защиты информации автоматизированных систем в соответствии с требованиями нормативной правовой и организационно-методической документации	ИПК-7.3. Осуществляет управление процессом защиты информации автоматизированных систем в соответствии с требованиями нормативной правовой и организационно-методической документации по защите информации ИПК-7.4. Осуществляет разработку, внедрение и контроль реализации правил и процедур управления системой защиты информации, работы с угрозами, инцидентами, автоматизированными системами и системами защиты информации

В результате изучения дисциплины обучающийся должен:

Знает:

– принципы и методы управления рисками информатизации бизнеса; классификацию рисков информатизации и методы их идентификации

– количественные методы оценки рисков информатизации бизнеса; методы обработки рисков и управления непрерывностью бизнеса

Умеет:

– организовывать и поддерживать выполнение мероприятий по управлению рисками информатизации бизнеса

– осуществлять количественную оценку рисков информатизации бизнеса и выбирать способы их обработки

Владеет:

– навыками управления процессом обеспечения информационной безопасности с учетом рисков информатизации бизнеса

– навыками разработки, внедрения и контроля реализации правил и процедур управления рисками информатизации бизнеса

1.2. Содержание дисциплины

№	Тема (раздел дисциплины) (в соответствии с РПД)	Код компетенции
	Тема 1. ИНФОРМАТИЗАЦИЯ БИЗНЕСА КАК ОБЪЕКТ УПРАВЛЕНИЯ РИСКАМИ	ОПК-10
	ТЕМА 2. КЛАССИФИКАЦИЯ РИСКОВ ИНФОРМАТИЗАЦИИ БИЗНЕСА	ОПК-10
	ТЕМА 3. ПРОЦЕСС УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАТИЗАЦИИ БИЗНЕСА	ОПК-10
	ТЕМА 4. КАЧЕСТВЕННЫЕ МЕТОДЫ ОЦЕНКИ РИСКОВ	ОПК-10
	ТЕМА 5. КОЛИЧЕСТВЕННЫЕ МЕТОДЫ ОЦЕНКИ РИСКОВ	ПК-7
	ТЕМА 6. МЕТОДЫ ОБРАБОТКИ РИСКОВ ИНФОРМАТИЗАЦИИ БИЗНЕСА	ПК-7
	ТЕМА 7. УПРАВЛЕНИЕ НЕПРЕРЫВНОСТЬЮ БИЗНЕСА	ПК-7
	ТЕМА 8. МОНИТОРИНГ И КОНТРОЛЬ РИСКОВ ИНФОРМАТИЗАЦИИ БИЗНЕСА	ПК-7

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.

Перечень вопросов 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. Информатизация бизнеса как объект управления рисками.
2. Понятие риска информатизации бизнеса, его составляющие.
3. Классификация рисков информатизации бизнеса.
4. Процесс управления рисками информатизации бизнеса: этапы и содержание.
5. Идентификация рисков информатизации бизнеса: источники и методы выявления.
6. Качественные методы оценки рисков информатизации бизнеса.
7. Реестр рисков информатизации бизнеса: назначение и порядок ведения.
8. Организация выполнения мероприятий по управлению рисками информатизации бизнеса.
9. Роль технического специалиста в процессе управления рисками информатизации бизнеса.
10. Взаимодействие процесса управления рисками информатизации с политикой информационной безопасности организации.

ПК-7. Способен организовать, поддерживать и управлять процессом защиты информации автоматизированных систем в соответствии с требованиями нормативной правовой и организационно-методической документации

1. Количественные методы оценки рисков информатизации бизнеса (ALE, ROI, ROSI).
2. Методы обработки рисков информатизации бизнеса: снижение, передача, принятие, уклонение.
3. Управление непрерывностью бизнеса (Business Continuity Management): понятие и принципы.
4. Планирование восстановления после инцидентов (Disaster Recovery Planning).
5. Разработка плана обеспечения непрерывности бизнеса.
6. Мониторинг и контроль рисков информатизации бизнеса.
7. Разработка правил и процедур управления рисками информатизации бизнеса.
8. Контроль реализации мероприятий по управлению рисками информатизации бизнеса.
9. Страхование информационных рисков как метод передачи риска.
10. Оценка экономической эффективности мероприятий по управлению рисками информатизации бизнеса.