Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Выборнова Любовь Александровна
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 Высшей школы интеллектуальных систем и кибертехнологий

Протокол от 11.10.2023 г. № 3

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

Б.1.О.03.26 «Проектирование комплексных систем безопасности»
наименование дисциплины

по образовательной программе высшего образования – программе **бакалавриата**

«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

Составители Сыротюк Светлана Дмитриевна, к.п.н., доцент, Высшая школа интеллектуальных систем и кибертехнологий
Мунирова Юлия Сергеевна, старший преподаватель, Высшая школа 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-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.
ОПК-12	Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	ИОПК-12.1. Знает порядок проектирования подсистем, средств обеспечения защиты информации. ИОПК-12.2. Формулирует требования и характеристики подсистем и средств обеспечения защиты информации для их последующего проектирования. ИОПК-12.3. Осуществляет подготовку исходных данных для технико-экономического обоснования проектных решений.

В результате изучения дисциплины обучающийся должен:

владеть: навыками составления политики безопасности, матрицы ответственности и плана реализации и контроля защитных мер; навыками подготовки проектных исходных данных, схем архитектуры, спецификаций и расчетов затрат на комплексную систему безопасности.

уметь: разрабатывать политику безопасности, распределять ответственность, планировать внедрение и сопровождение комплекса защитных мер; проводить обследование объекта, формировать модель угроз, требования и техническое задание, сравнивать проектные варианты.

знать: принципы комплексной защиты, содержание политики информационной безопасности, взаимосвязь организационных, физических и технических мер; этапы проектирования, состав исходных данных, требования к подсистемам безопасности и способы технико-экономического обоснования решений

1.2. Содержание дисциплины

№	Тема (раздел дисциплины) (в соответствии с РПД)	Код компетенции
1	Обследование объекта и исходные данные для проектирования	ОПК-10 ОПК-12
2	Модель угроз и оценка рисков безопасности	ОПК-10 ОПК-12
3	Политика безопасности и требования к комплексной системе	ОПК-10 ОПК-12
4	Архитектура комплексной системы и интеграция подсистем	ОПК-10 ОПК-12
5	Проектирование физической и инженерно-технической защиты	ОПК-10 ОПК-12
6	Проектирование защиты информационной инфраструктуры	ОПК-10 ОПК-12
7	Технико-экономическое обоснование и проектная документация	ОПК-10 ОПК-12
8	Внедрение, испытания и сопровождение комплексной системы	ОПК-10 ОПК-12

1.3. Система оценивания по дисциплине

Дисциплина изучается в течение одного семестра

Форма промежуточной аттестации по дисциплине — экзамен

Шкалы оценки уровня сформированности результатов обучения		Шкала оценки уровня освоения дисциплины		
Уровневая шкала оценки компетенций	100 бальная шкала, %	100 бальная 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

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в ходе текущего контроля успеваемости (в процессе проведения лабораторных и практических занятий, тематических опросов и выполнения курсовой работы).

В ходе проведения промежуточной аттестации осуществляется контроль и оценка результатов освоения компетенций.

Перечень вопросов и заданий 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 комплексной системы безопасности и взаимосвязь ее подсистем.
2. Цели и область действия политики информационной безопасности.

3. Принципы многоуровневой защиты и минимальных привилегий.
4. Распределение ролей, полномочий и ответственности за безопасность.
5. Управление физическим доступом и доступом к информационным ресурсам.
6. Согласование организационных и технических мер защиты.
7. Планирование внедрения комплекса защитных мер.
8. Управление изменениями конфигурации системы безопасности.
9. Организация регистрации и анализа событий безопасности.
10. Взаимодействие подсистем контроля доступа, сигнализации и мониторинга.
11. Организация резервного копирования и восстановления.
12. Планирование действий при отказе защитной подсистемы.
13. Показатели выполнения и эффективности защитных мер.
14. Порядок пересмотра политики безопасности и реестра рисков.
15. Регламенты эксплуатации и обслуживания комплекса.
16. Критерии приемки и документирование результатов испытаний.
17. Остаточный риск и порядок согласования его принятия.
18. Обоснование выбора мер с учетом условий эксплуатации.
19. Требования к совместимости подсистем и средств защиты.
20. Прослеживаемость угроз, требований, мер и контрольных процедур.

ОПК-12. Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений

1. Этапы проектирования комплексной системы безопасности.
2. Обследование объекта и состав исходных данных.
3. Инвентаризация и классификация активов.
4. Построение схем потоков данных и границ доверия.
5. Разработка модели нарушителя и модели угроз.
6. Качественная оценка вероятности, ущерба и приоритетов риска.
7. Функциональные и эксплуатационные требования к системе.
8. Состав технического задания на комплексную систему.
9. Зонирование территории, помещений и информационной инфраструктуры.
10. Выбор архитектуры и интерфейсов взаимодействия подсистем.
11. Подготовка исходных данных для выбора физических мер защиты.
12. Подготовка исходных данных для защиты от технических каналов утечки.
13. Подготовка исходных данных для сегментации сети и управления доступом.
14. Выбор показателей надежности и восстановления.
15. Состав спецификации оборудования, программных средств и работ.
16. Единовременные и эксплуатационные затраты проектного решения.
17. Методы сравнения альтернативных вариантов проекта.
18. Анализ чувствительности затрат к изменению исходных данных.
19. Состав проектной и эксплуатационной документации.
20. Порядок обоснования решений и защиты курсовой работы.