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:
c3b3b9c625f6c113afa2a2c42ba...

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 10.11.2023 № 3

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

Б.1.В.03.10 «Организация защиты персональных данных»
наименование дисциплины

по образовательной программе высшего образования – программе **бакалавриат**

«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 Коновалова Анжелика Денисовна, 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-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. ИОПК-6.2. Знает и применяет положения действующих в РФ нормативных правовых актов, нормативных и методических документов по вопросам организации защиты информации ограниченного доступа.
ПК-1	Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	ИПК-1.1. Устанавливает, настраивает и обслуживает программное обеспечение, программно-аппаратные и технические средства защиты информации с соблюдением требований по защите информации ИПК-1.2. Умеет устанавливать программное обеспечение в соответствии с технической документацией, выполнять настройку параметров работы программного обеспечения, включая системы управления базами данных и средства электронного документооборота, формулировать правила безопасной эксплуатации

В результате изучения дисциплины обучающийся должен:

владеть: навыками составления реестра процессов обработки, описания угроз и нарушителей, документирования мер защиты, планирования контроля, организации реагирования на инциденты и подготовки доказательств выполнения требований по защите персональных данных

уметь: обследовать процессы обработки персональных данных; определять состав защищаемых сведений и границы ИСПДн; обосновывать применимые требования, уровень защищенности и набор мер; разрабатывать локальные документы и правила доступа; проверять выполнение мер на учебном примере

знать: правовые основания и принципы обработки персональных данных; права субъектов и обязанности оператора; требования к организации защиты персональных данных при автоматизированной и неавтоматизированной обработке; порядок определения угроз и уровней защищенности, выбора организационных и технических мер защиты

1.2. Содержание дисциплины

№	Тема (раздел дисциплины) (в соответствии с РПД)	Код компетенции
1	Персональные данные как объект защиты. Нормативное регулирование	ОПК-6 ПК-1
2	Правовые основания обработки и обеспечение прав субъектов	ОПК-6 ПК-1
3	Обследование процессов обработки и организация системы защиты	ОПК-6 ПК-1
4	Моделирование угроз и определение уровня защищенности ИСПДн	ОПК-6 ПК-1
5	Выбор организационных и технических мер защиты персональных данных	ОПК-6 ПК-1
6	Защита при неавтоматизированной обработке, передаче и хранении данных	ОПК-6 ПК-1
7	Эксплуатация системы защиты и реагирование на инциденты	ОПК-6 ПК-1
8	Контроль выполнения требований и совершенствование защиты персональных данных	ОПК-6 ПК-1

1.3. Система оценивания по дисциплине

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

Уровень сформированности	100-балльная шкала, %	Шкала освоения, %	5-балльная дифференцированная оценка/балл
допороговый	ниже 61	ниже 61	не зачтено
пороговый	61–85,9	61–69,9	зачтено
пороговый	61–85,9	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: практических занятий, тестирования, опросов, проверки самостоятельной работы.

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

Перечень вопросов и заданий для подготовки к зачету

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 персональных данных. Идентификация субъекта по прямым и косвенным признакам. Приведите примеры спорных случаев.
2. Оператор и лицо, осуществляющее обработку по поручению. Распределение обязанностей и ответственности.
3. Категории персональных данных. Условия отнесения сведений к специальным категориям и биометрическим данным.
4. Автоматизированная и неавтоматизированная обработка: признаки и применимые требования к защите.
5. Система нормативного регулирования. Полномочия Роскомнадзора, ФСТЭК России и ФСБ России.
6. Принципы обработки персональных данных. Проверка соответствия состава данных цели обработки.
7. Правовые основания обработки данных работника и клиента. Случаи обработки без согласия.
8. Согласие на обработку персональных данных: содержание, доказуемость, отдельное оформление и отзыв.
9. Обработка данных, разрешенных субъектом для распространения. Отличие от предоставления определенному получателю.
10. Права субъекта и порядок рассмотрения обращения. Проверка полномочий заявителя и документирование ответа.
11. Уведомление об обработке персональных данных и поддержание сведений об операторе в актуальном состоянии.
12. Поручение обработки, локализация и трансграничная передача. Разграничение требований и проверяемые документы.
13. Обследование процессов обработки. Состав исходных данных и методы выявления неучтенных копий.
14. Границы ИСПДн и ее состав. Учет внешних сервисов, удаленного доступа и резервных копий.
15. Реестр процессов обработки и схема потоков данных. Назначение и взаимосвязь документов.
16. Ответственный за организацию обработки и ответственный за безопасность данных. Разделение функций.
17. Политика обработки персональных данных и внутренние локальные акты. Порядок утверждения и актуализации.
18. Обучение и допуск персонала к обработке. Подтверждение ознакомления и контроль соблюдения правил.
19. Модель угроз ИСПДн: назначение, исходные данные, структура и основания пересмотра.

20. Модель нарушителя: внутренние и внешние нарушители, возможности и условия доступа.

21. Связь активов, уязвимостей, угроз и негативных последствий. Обоснование актуальности угрозы.

22. Применение банка данных угроз ФСТЭК России. Почему выгрузка банка не заменяет модель угроз?

23. Типы угроз по постановлению Правительства РФ № 1119 и их учет при выборе уровня защищенности.

24. Критерии определения уровня защищенности ИСПДн. Документирование исходных данных и решения.

25. Порядок выбора организационных и технических мер: базовый набор, адаптация, уточнение, дополнение.

26. Идентификация, аутентификация и управление доступом. Принципы минимальных привилегий и разделения обязанностей.

27. Учетные записи и матрица доступа. Выдача, пересмотр и отзыв полномочий.

28. Регистрация событий безопасности. Состав событий, защита журналов и организация анализа.

29. Защита от вредоносного программного обеспечения, анализ защищенности и управление обновлениями.

ПК-1. Способен выполнять работы по установке, настройке и обслуживанию программных, программно- аппаратных (в том числе криптографических) и технических средств защиты информации

30. Криптографическая защита персональных данных: условия применения, выбор средств и организация эксплуатации.

31. Требования к неавтоматизированной обработке. Обособление данных, типовые формы и доступ к местам хранения.

32. Учет, хранение и передача бумажных документов и машинных носителей. Контроль выдачи и возврата.

33. Передача персональных данных по сети: проверка получателя, минимизация состава и выбор мер защиты.

34. Организация защиты при удаленной работе и использовании услуг подрядчика.

35. Хранение, блокирование, удаление и уничтожение данных. Подтверждающие документы и учет копий.

36. Обезличивание, шифрование и уничтожение: различия целей, результатов и ограничений.

37. Эксплуатационный контроль системы защиты. Учет изменений и периодический пересмотр мер.

38. Признаки инцидента безопасности и первичные действия работника. Регистрация и эскалация.

39. Сохранение доказательств при расследовании инцидента. Источники, целостность и ограничение доступа.

40. Обязанности оператора при нарушении прав субъектов вследствие неправомерной или случайной передачи данных.

41. Содержание первичного и дополнительного уведомлений об инциденте. Определение сроков по действующему закону.

42. Восстановление после инцидента, устранение причин и проверка корректирующих мер.

43. Оценка эффективности мер до ввода ИСПДн в эксплуатацию. Критерии и подтверждающие материалы.

44. Программа внутреннего контроля. Документальная проверка, интервью, технические свидетельства и выборка.

45. Оформление несоответствия и план корректирующих мероприятий. Проверка закрытия нарушения.

46. Внутренний контроль, оценка эффективности и аттестация: цели и границы применимости.

47. Подготовка документов и доказательств выполнения требований для взаимодействия с уполномоченным органом.

48. Согласованность реестра процессов, модели угроз, уровня защищенности, мер защиты и локальных актов.