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 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.03.18 «Защита информации от утечки по техническим каналам»
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-9	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ИОПК-9.2. Применяет средства криптографической и технической защиты информации от «утечки».
ПК-4	Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств защиты информации в автоматизированных системах	ИПК-4.1. Применяет программные, программно-аппаратные и технические средства защиты информации автоматизированных систем, в том числе криптографические методы, алгоритмы и протоколы. ИПК-4.2. Осуществляет конфигурирование параметров программных, программно-аппаратных и технических средств защиты информации автоматизированных систем.

В результате изучения дисциплины обучающийся должен:

владеть навыками: навыками применения средств технической защиты информации и оценки эффективности принятых мер; навыками конфигурирования средств защиты, проведения контрольных измерений и оформления результатов.

уметь: выявлять возможные технические каналы утечки, определять условия их реализации и выбирать адекватные меры защиты; выбирать, устанавливать и настраивать средства защиты с учетом характеристик объекта информатизации.

знать: виды технических каналов утечки информации, физические основы их образования, методы и средства технической защиты информации; назначение, состав и параметры программно-аппаратных и технических средств защиты информации от утечки по техническим каналам.

1.2. Содержание дисциплины

№	Тема (раздел дисциплины) (в соответствии с РПД)	Код компетенции
1.	Технические каналы утечки и модель угроз	ОПК-9 ПК-4
2.	Акустические и виброакустические каналы	ОПК-9 ПК-4
3.	Побочные электромагнитные излучения и наводки	ОПК-9 ПК-4
4.	Оптико-электронные и визуальные каналы	ОПК-9 ПК-4
5.	Каналы утечки по цепям питания, заземления и линиям связи	ОПК-9 ПК-4
6.	Обследование объекта и специальные проверки	ОПК-9 ПК-4
7.	Средства защиты от утечки по техническим каналам	ОПК-9 ПК-4
8.	Контроль эффективности и документирование	ОПК-9 ПК-4

1.3. Система оценивания по дисциплине

Дисциплина изучается в течение одного семестра.

Форма промежуточной аттестации по дисциплине – зачет.

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 практических занятий, тестирования, опросов).

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

Перечень вопросов и заданий для подготовки к зачету

ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности

1. Понятие технического канала утечки информации и его основные элементы.
2. Классификация технических каналов утечки информации.
3. Источники и носители защищаемой информации на объекте информатизации.
4. Контролируемая зона: назначение и принципы установления границ.
5. Модель нарушителя применительно к техническим каналам утечки.
6. Модель угроз утечки информации по техническим каналам.
7. Физические основы образования акустического канала утечки.
8. Физические основы образования виброакустического канала утечки.
9. Факторы, влияющие на распространение речевого сигнала через ограждающие конструкции.
10. Пассивные способы защиты речевой информации.
11. Активные способы акустической и виброакустической защиты.
12. Причины возникновения побочных электромагнитных излучений и наводок.
13. Источники опасных сигналов в технических средствах обработки информации.
14. Зоны возможного перехвата побочных электромагнитных излучений.
15. Экранирование как способ снижения уровня информативных излучений.
16. Оптико-электронные и визуальные каналы утечки информации.
17. Условия применения средств оптического наблюдения и лазерных систем съема информации.
18. Способы защиты информации от визуального наблюдения.
19. Утечка информации по цепям электропитания.
20. Утечка информации по цепям заземления.
21. Паразитные связи и взаимные наводки в кабельных системах.
22. Фильтрация и развязка цепей как меры технической защиты.

23. Требования к организации защитного заземления.
24. Этапы обследования объекта информатизации.
25. Инвентаризация технических средств и коммуникаций объекта.
26. Выбор опасных направлений и контрольных точек.
27. Назначение и структура программы специальной проверки.
28. Основные группы средств технической защиты информации.
29. Методы контроля эффективности технической защиты.
30. Критерии достаточности защиты информации от утечки по техническим каналам.

ПК-4. Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств защиты информации в автоматизированных системах

1. Порядок выявления технических каналов утечки на объекте информатизации.
2. Подготовка исходных данных для выбора средств технической защиты.
3. Выбор мер защиты с учетом характеристик помещения и контролируемой зоны.
4. Принципы установки и размещения средств акустической защиты.
5. Настройка генераторов акустического и виброакустического шума.
6. Проверка работоспособности средств акустической защиты.
7. Выбор технических мер защиты от побочных электромагнитных излучений.
8. Организация экранирования помещений, оборудования и кабельных линий.
9. Порядок применения сетевых фильтров и развязывающих устройств.
10. Конфигурирование параметров средств активной технической защиты.
11. Контроль безопасных режимов эксплуатации средств защиты.
12. Определение контрольных точек при проведении измерений.
13. Требования к подготовке измерительной аппаратуры.
14. Учет фоновых помех при проведении контрольных измерений.
15. Оценка результатов измерений и сопоставление с установленными критериями.
16. Порядок документирования параметров настройки средств защиты.
17. Разработка схемы размещения средств технической защиты.
18. Учет электромагнитной совместимости при выборе средств защиты.
19. Организация защиты выделенного помещения.
20. Организация защиты технических средств обработки информации.
21. Меры защиты кабельной инфраструктуры объекта информатизации.
22. Порядок проведения специального обследования помещения.
23. Порядок проведения проверки линий электропитания и заземления.
24. Порядок проверки окон, дверей и инженерных коммуникаций.
25. Выявление неучтенных технических средств и коммуникаций.
26. Оценка достаточности выбранного комплекса технических мер.
27. Разработка корректирующих мер по результатам контроля.
28. Содержание акта контроля эффективности технической защиты.
29. Требования к технической документации на применяемые средства защиты.
30. Обслуживание и периодический контроль средств защиты информации.