

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Выборнова Любовь Алексеевна
Должность: Ректор
Дата подписания: 28.07.2026 09:33:10
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 02.12.2022г. № 4

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

«Управление информационной безопасностью»

наименование дисциплины

по образовательной программе высшего образования – программе

магистратуры

бакалавриата, специалитета,
магистратуры

«Информационная безопасность интеллектуальных и информационно-аналитических систем»

наименование образовательной программы

10.04.01 «Информационная безопасность»

шифр, наименование направления подготовки / специальности

Составитель Глухова Л.В., профессор, Высшая школа
интеллектуальных систем и кибертехнологий,
д.э.н., профессор
ФИО, должность, структурное подразделение,
ученая степень, ученое звание

Тольятти
2022

1. Паспорт фонда оценочных средств (далее – ФОС)

1.1. Планируемые результаты обучения по дисциплине

Код компетенции	Наименование компетенции	Код и наименование индикаторов достижения компетенции
УК-3.	Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	ИУК-3.2. Осуществляет принятие исполнительских решений в условиях спектра мнений, определение порядка выполнения заданий
ОПК-1.	Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	ИОПК-1.1. Понимает принципы, требования и структуру системы обеспечения информационной безопасности и защиты информации ИОПК-1.2. Проектирует техническое задание на создание системы обеспечения информационной безопасности и защиты информации
ОПК-3.	Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности	ИОПК-3.1. Применяет нормативные правовые акты, методические документы при подготовке распорядительных документов по обеспечению информационной безопасности, в том числе при разработке ИАС ИОПК-3.2. Разрабатывает проекты организационно-распорядительных документов по обеспечению информационной безопасности

В результате изучения дисциплины обучающийся должен:

Владеть:

- навыками принятия исполнительских решений в условиях спектра мнений и порядка выполнения работ по управлению информационной безопасностью
- навыками проектирования систем обеспечения информационной безопасности
- навыками работы с нормативными документами ФСТЭК при управлении информационной безопасностью.

Уметь:

- планировать стратегию членов команды по обеспечению информационной безопасности
- разрабатывать техническое задание на создание системы обеспечения информационной безопасности и защиты информации
- разрабатывать проекты информационно-аналитических систем и организационно-распорядительных документов по обеспечению информационной безопасности

Знать:

- основные функции организации и управления работой команды исполнителей
- принципы обеспечения информационной безопасности и защиты информации и требования нормативных документов для разработки проекта технического задания
- принципы проектирования и разработки организационно-распорядительных документов по обеспечению информационной безопасности и требования нормативной базы ФСТЭК

1.2. Содержание дисциплины

№	Тема (раздел дисциплины) (в соответствии с РПД)	Код компетенции
1	Тема 1. Основные понятия науки об управлении. Системный, процессный, нормативный подходы	УК-3 ОПК-1
2	Тема 2. Проектирование системы управления информационной безопасностью на предприятии	ОПК-1 ОПК-3
3	Тема 3. Оценка рисков информационной безопасности на предприятии	УК-3; ОПК-1 ОПК-3

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 балльная шкала, %	100 балльная 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 для подготовки к экзамену

УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели

1. Какой документ регламентирует обеспечение правовых условий использования электронной цифровой подписи в электронных документах?
2. Что является основным документом, обеспечивающим защиту персональных данных?
3. Под какую статью УК РФ попадает такое киберпреступление, как неправомерный доступ к компьютерной информации?
4. Дайте определение понятия «Критерий экономической безопасности - это»
5. Какой государственный стандарт содержит «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер»?
6. Дайте определение информационной безопасности.
7. В виде совокупности каких уровней можно представить организационную структуру системы обеспечения информационной безопасности АС организации?
8. Дайте определение понятия «Система защиты информации (СЗИ)»
9. Дайте определение понятия «Профессиональная тайна»
10. В чём разница между служебными и коммерческими секретами?
11. Дайте определение понятия «Персональные данные»
12. Какими факторами могут быть обусловлены информационные угрозы?
13. Запишите виды информационных угроз для государства
14. Запишите виды информационных угроз для компании.
15. Запишите виды информационных угроз для личности (физического лица).
16. Дайте определение Макровируса
17. Дайте определение экономической безопасности
18. Какой документ устанавливает классификацию и перечень факторов, воздействующих на безопасность защищаемой информации, в целях обоснования угроз безопасности информации и требований по защите информации на объекте информатизации
19. Какой орган впервые определил критерии установления коммерческого мошенничества.
20. Закончите определение. Согласно Стратегии экономической безопасности РФ до 2030 года угрозы экономической безопасности – это...

ОПК-1.. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание

1. Перечислите функции, выполняемые антивирусом Касперского.
2. Дайте краткую характеристику антивирусам сканерам
3. Дайте краткую характеристику антивирусам мониторам

4. Запишите меры профилактики заражения ПК вирусом.
5. Запишите основные пути проникновения вирусов на компьютер
6. Перечислите вредные действия вирусов.
7. Дайте определение понятия «Персональные данные»
8. Какими факторами могут быть обусловлены информационные угрозы?
9. Запишите виды информационных угроз для государства
10. Запишите виды информационных угроз для компании
11. Запишите виды информационных угроз для личности (физического лица)
12. Дайте определение Макровируса
13. Макровирусы заражают файлы – документы и электронные таблицы офисных приложений. Для анализа макровирусов необходимо получить текст их макросов. При помощи, каких команд можно это сделать для нешифрованных (не-стелс) файлов?
14. Если на компьютере нет антивирусных программ, то каким образом можно восстановить документы Word и Excel заражённых вирусом?
15. Запишите последовательность действий, которые необходимо выполнить для того, чтобы восстановить пораженные документы Word и Excel в случае того, если на компьютере нет антивирусных программ
16. Запишите, какие действия необходимо выполнить, для защиты файлов от макровирусов, если на компьютере нет антивирусных программ.
17. Запишите виды информационных угроз для государства.
18. Какие действия необходимо выполнить в MS Office чтобы зашифровать файл и задать пароль для его открытия?
19. Запишите алгоритм процесса создания архива с паролем в WinRAR. и архив будет создан с паролем.
20. Расшифруйте слово «экпёяёнро», закодированное с помощью шифра Цезаря. Известно, что каждая буква исходного текста заменяется третьей после нее буквой.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	
3	Расшифруйте: э к п ё я ё н р о																																
4																																	
5	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я

ОПК-3. Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности

1. Какие особенности проектирования и разработки организационно-распорядительных документов по обеспечению ИБ регламентированы ГОСТ Р ИСО /МЭК 27005-2010
2. Соотнести между собой процессы системы менеджмента информационной безопасности и процесса менеджмента риска информационной безопасности
3. Что должно быть реализовано в организации при управлении контентом. В соответствии с требованиями ГОСТ Р ИСО/МЭК 27005-2010
4. Перечислить в качестве примера цели менеджмента риска информационной безопасности, которые могут быть указаны в документе «Руководство по реализации» (ГОСТ Р ИСО/МЭК 27005-2010)
5. С учетом чего рекомендовано в организации формировать критерии оценки рисков ИБ?
6. Что такое идентификация риска и какова цель идентификации
7. Роль организационной структуры менеджмента риска информационной безопасности
8. Общее описание оценки риска ИБ

9. Как происходит определение активов организации для их защиты от рисков?
10. Привести пример того, в каких областях деятельности организации могут быть выявлены уязвимости
11. Привести пример последствий, которые могут быть вызваны потерей конфиденциальности, целостности и доступности
12. Привести пример, на основе чего организации могут определять операционные последствия выявленного сценария компьютерного инцидента?
13. В чем заключается управление информационной безопасностью в организации
14. Чем занимается отдел информационной безопасности в организации и что входит в его основные задачи?
15. Каково назначение процесса управления информационной безопасностью организации с точки зрения процессного подхода?
16. Назовите предпосылки разработки политики безопасности предприятия