

МИНОБРАЗОВАНИЯ РОССИИ
ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

**РАБОЧАЯ ПРОГРАММА
УЧЕБНОЙ ДИСЦИПЛИНЫ**

*МДК.06.02 Инженерно-техническая поддержка сопровождения
информационных систем*

программы подготовки специалистов среднего звена /
квалифицированных рабочих и служащих

09.02.07 Информационные системы и программирование

Форма обучения: *очная*

Находка 2026

Рабочая программа учебной дисциплины *МДК.06.02 Инженерно-техническая поддержка сопровождения информационных систем* разработана в соответствии с требованиями Федерального государственного образовательного стандарта среднего профессионального образования по специальности / профессии *09.02.07 Информационные системы и программирование*, утвержденного приказом Минобрнауки России от «09» декабря 2016 г. № 1547, примерной образовательной программой.

Разработчик(и): *Лихацкий М.Б. преподаватель ОСПО филиала ФГБОУ ВО «ВВГУ» в г. Находке*

Рассмотрено и одобрено на заседании цикловой методической комиссии

Протокол № 10 от «29» июня 2026 г.

Председатель ЦМК _____ *В.В Плахотина*
подпись

Содержание

- 1 ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ
УЧЕБНОЙ ДИСЦИПЛИНЫ**
- 2 СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ**
- 3 УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ**
- 4 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ
УЧЕБНОЙ ДИСЦИПЛИНЫ**

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

1.1 Место дисциплины в структуре основной образовательной программы

Учебная дисциплина *МДК.06.02 Инженерно-техническая поддержка сопровождения информационных систем* является частью учебного цикла основной образовательной программы (далее ООП) в соответствии с ФГОС СПО по специальности/профессии *09.02.07 Информационные системы и программирование*.

1.2 Цель и планируемые результаты освоения дисциплины

По итогам освоения дисциплины, обучающиеся должны продемонстрировать результаты обучения, соотнесённые с результатами освоения ООП СПО, приведенные в таблице.

Код компетенции	Умения	Знания
ОК 1 ОК 2	Выполнять резервное копирование и восстановление данных информационных систем (ИС). Настраивать и администрировать ИС в соответствии с регламентами.	Виды и методы резервного копирования, политики восстановления (RTO, RPO). Организацию сопровождения ИС, ролевые функции, договоры на сопровождение.
ОК 4 ОК 5	Проводить мониторинг и диагностику работоспособности ИС. Обеспечивать безопасность функционирования ИС (управление доступом, установка обновлений).	Регламенты обновления ПО и обеспечения безопасности. Методы и инструменты диагностики, мониторинга производительности и выявления ошибок.
ОК 9 ОК 10	Идентифицировать и устранять ошибки в работе ИС. Составлять отчёты об ошибках и техническую документацию.	Состав пользовательской и технической документации (руководство программиста, администратора). Основы безопасности ИС, методы защиты от НСД. Инструментальные средства для администрирования и мониторинга.
ПК 5.1 ПК 5.2 ПК 5.6 ПК 6.3	Собирать исходные данные для разработки проектной документации на информационную систему. Разрабатывать проектную документацию на разработку информационной системы в соответствии с требованиями заказчика. Разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием. Производить разработку модулей информационной системы в соответствии с техническим заданием.	Инструментальные средства информационных технологий. Методологии разработки и сопровождения ИС. Этапы жизненного цикла ИС, процессы управления изменениями. Требования к проектной документации, стандарты оформления.

2 Структура и содержание учебной дисциплины

2.1 Объем учебной дисциплины и виды учебной работы

Таблица 2 - Распределение трудоемкости дисциплины по видам учебной работы

Вид учебной работы	Объем часов
Объем образовательной программы учебной дисциплины	54
в том числе:	
– теоретическое обучение	18
– практические занятия (<i>если предусмотрено</i>)	34
– самостоятельная работа	
– консультации	
– промежуточная аттестация – (<i>дифференцируемый зачет</i>)	2

2.2 Тематический план и содержание учебной дисциплины «МДК.06.02 Инженерно-техническая поддержка сопровождения информационных систем»

Таблица 3 - Тематический план дисциплины

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем часов	Коды компетенций, формированию которых способствует элемент программы
1	2	3	4
Введение	Введение. История возникновения и развития информационных систем. Связь с другими дисциплинами и области применения информационных систем. Назначение электронно-вычислительной техники в информационных системах.	2	ОК 1, ОК 2, ОК 4, ОК 5, ОК 9, ОК 10, ПК 5.1, 5.2, 5.6, ПК 6.3
Раздел 1. Инженерно-техническая поддержка сопровождения информационных систем		50	
Тема 1.1 Организация сопровождения и восстановления работоспособности системы	Содержание учебного материала: Задачи сопровождения информационной системы. Ролевые функции и организация процесса сопровождения. Сценарий сопровождения. Договор на сопровождение. Анализ исходных программ и компонентов программного средства. Программная инженерия и оценка качества. Реинжиниринг. Цели и регламенты резервного копирования. Сохранение и откат рабочих версий системы. Сохранение и восстановление баз данных	4	ОК 1, ОК 2, ОК 4, ОК 5, ОК 9, ОК 10, ПК 5.1, 5.2, 5.6, ПК 6.3
	Практическая работа №1: «Разработка плана резервного копирования» Практическая работа №2: «Создание резервной копии информационной системы»	10	

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем часов	Коды компетенций, формированию которых способствует элемент программы
1	2	3	4
Тема 1.2. Администрирование и безопасность информационной системы	Содержание учебного материала: Организация процесса обновления в информационной системе. Регламенты обновления. Обеспечение безопасности функционирования информационной системы. Организация доступа пользователей к информационной системе	6	ОК 1, ОК 2, ОК 4, ОК 5, ОК 9, ОК 10, ПК 5.1, 5.2, 5.6, ПК 6.3
	Практическая работа №3: «Восстановление данных» Практическая работа №4: «Восстановление работоспособности системы» Практическая работа №5: «Создание резервной копии базы данных»	12	
	Самостоятельная работа обучающихся	Не предусмотрено	
	Лабораторное занятие	Не предусмотрено	
Тема 1.3 Идентификация и устранение ошибок в информационной системе	Содержание учебного материала: Организация сбора данных об ошибках в информационных системах. Системы управления производительностью приложений. Мониторинг сетевых ресурсов. Схемы и алгоритмы анализа ошибок. Отчет об ошибках системы: содержание, использование информации. Пользовательская документация: «Руководство программиста», «Руководство системного администратора». Выявление аппаратных ошибок информационной системы. ~~Техническое обслуживание аппаратных средств~~	6	ОК 1, ОК 2, ОК 4, ОК 5, ОК 9, ОК 10, ПК 5.1, 5.2, 5.6, ПК 6.3
	Практическая работа №6: «Сбор информации об ошибках. Формирование отчетов об ошибках». Практическая работа №7: «Выявление и устранение ошибок программного кода информационных систем». Практическая работа №8: «Выполнение обслуживания информационной системе в соответствии с пользовательской документацией».	12	
	Самостоятельная работа обучающихся	Не предусмотрено	
	Лабораторное занятие	Не предусмотрено	
Промежуточная аттестация - дифференцированный зачет		2	

ИТОГО часов		54	
Теоретические занятия		18	
Практические занятия		34	
Самостоятельная работа		0	
Дифференцированный зачет		2	

3 Условия реализации учебной дисциплины

3.1 Для реализации программы учебной дисциплины «МДК.06.02 Инженерно-техническая поддержка сопровождения информационных систем» образовательной организации, предусмотрено наличие следующих специальных помещений:

Для реализации программы учебной дисциплины предусмотрено наличие следующих специальных помещений:

Компьютерный класс информационных технологий: количество посадочных мест - 28 шт., доска меловая - 1 шт., стол для преподавателя - 1 шт., стул для преподавателя - 1 шт.; учебно-методические пособия, дидактические и презентационные материалы

Компьютерный класс имеет следующее оборудование:

Учебно-лабораторное оборудование: Процессор Intel Количество ядер - 2 . Объем кэш-памяти - 8Мб • Базовая частота процессора - 2,0 ГГц. Объем установленной памяти - 4Гб Накопитель твердотельный объемом 512 видео карта - встроенная. Максимальное разрешение - 1920x1080 пикс. Диагональ монитора 23" количество мониторов 1 шт. Разрешение: FHD (1920x1080 пикс.) клавиатура мышь ОС Microsoft Windows 7 Pro Мультимедийный комплект в составе: проектор Sanyo, крепление Kromax, экран Lumien Eco Picture: Технология проецирования изображения - микрозеркала на полупроводниковом чипе. Базовое разрешение проектора: 1280x800 пикс. Входы - VGA, HDMI 2 шт., Порты - RS-232C, USB 2 шт., LAN Размер полотна: ширина 200 см, высота 127 см. ПО: Microsoft Office 2010, Пакет Adobe CC 2019, Pixologic Zbrush Academic Volume License, Adobe Substance Painter, Autodesk 3Ds max, Maya, Blender, Unity, Unreal Engine

3.2 Информационное обеспечение реализации программы

Для реализации программы учебной дисциплины библиотечный фонд ВВГУ укомплектован печатными и электронными изданиями.

Обучающиеся из числа инвалидов и лиц с ограниченными возможностями здоровья обеспечены печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

Основная литература:

1. Бизяев, А.А. Информационные технологии: практикум: [Электронный ресурс]/А.А. Бизяев, К.А. Куратов ; Новосибирский государственный технический университет. - Новосибирск: Новосибирский государственный технический университет, 2022. - 96 с.: ил., табл. - Режим доступа: <http://biblioclub.ru/index.php?page=book&id=575330>

2. Информационные технологии [Электронный ресурс] : метод. рекомендации по самостоят. изучению дисциплины / Г.И. Попов, С.И. Бажинов, В.Г. Конюхов, Е.Н. Яшкина, В.А. Пирогов .- М. : РГУФКСМиТ, 2022 .-167 с. : ил. - Режим доступа: <https://lib.rucont.ru/efd/671375>

3. Информационные технологии в профессиональной деятельности [Электронный ресурс] / Т.В. Марзаева .— Улан-Удэ : Бурятский государственный университет, 2025 .- 71 с. -Режим доступа: <https://lib.rucont.ru/efd/348195>

4. Информационные технологии: учеб. пособие [Электронный ресурс]/ Л.Г. Гагарина, Я.О. Теплова, Е.Л. Румянцева, А.М. Баин / под ред. Л.Г. Гагариной. — Москва: ИД «ФОРУМ»: ИНФРА- М, 2021. — 320 с. -Режим доступа: <https://znanium.com/catalog/product/471464>.

5. Филимонова, Е.В. Информационные технологии в профессиональной деятельности : учебник / Филимонова Е.В. — Москва : КноРус, 2022. — 482 с. — (СПО). — ISBN 978-5-406-04887-0. — URL: <https://book.ru/book/922139> (дата обращения:

06.08.2024). — Текст : электронный.

6. Хныкина, А.Г. Информационные технологии [Электронный ресурс] : учеб. пособие / Т.В. Минкина, А.Г. Хныкина .— Ставрополь : изд-во СКФУ, 2023 .— 126 с. : ил. — Режим доступа: <https://lib.rucont.ru/efd/671178>

Дополнительная литература:

1. Богданова, С.В. Информационные технологии [Электронный ресурс]: учебное пособие / С.В. Богданова, А.Н. Ермакова. - Ставрополь: Сервисшкола, 2024. - 211 с. - Режим доступа: <https://znanium.com/catalog/product/514867>

2. Самойленко, А.П. Информационные технологии статистической обработки данных [Электронный ресурс] : учеб. пособие / О.А. Усенко, Южный федеральный ун-т, А.П. Самойленко .— Ростов н/Д. : Изд-во ЮФУ, 2024 .— 128 с. : ил. — ISBN 978-5-9275-2521-8 .— Режим доступа: <https://lib.rucont.ru/efd/692393>

3. Суханова, О.Н. Информационные технологии [Электронный ресурс] : лаб. практикум / О.В.

4. Ментюкова, О.Н. Суханова .— Пенза : РИО ПГСХА, 2022 .- 116 с. : ил. - Режим доступа: <https://lib.rucont.ru/efd/323727>.

Интернет-ресурсы:

1. www.informatics.mccme.ru/moodle/ - дистанционная подготовка по информатике.
2. www.ixbt.com - сайт о высоких технологиях, новости индустрии из мира компьютерного «железа», тестовые испытания и обзоры оборудования. Конференция. Платформа ПК. Цифровой звук. Цифровое фото. Мобильные устройства. Форум.
3. www.lib.ru/INTERMET/termwww.txt - толковый словарь терминов.
4. www.computerra.ru - новости про компьютеры, железо, новые технологии, информационные технологии. Рубрики: В поле зрения; Компьютерралаб; Дюжина полезных программ; Реклама на сайте; Блоги; Наука и жизнь. Архив номеров журнала.
5. www.novtex.ru/IT/arhiv.htm
6. <https://www.planttext.com/>
7. <https://kroki.io/#>
8. <https://www.canva.com/ru ru/>
9. <https://prezi.com/>
10. www.jir.ru/ - электронный научный журнал.

4. Контроль результатов освоения учебной дисциплины

Результаты обучения	Критерии оценки	Методы оценки
- актуальный профессиональный и социальный контекст, в котором приходится работать и жить; - основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; - алгоритмы выполнения работ в профессиональной и смежных областях; - методы работы в профессиональной и смежных сферах; - структуру плана для решения задач; - порядок оценки результатов решения задач профессиональной деятельности - основные методы и средства сбора, обработки, хранения, передачи и накопления информации; - технологию поиска информации в сети Интернет; - номенклатура информационных источников применяемых в профессиональной деятельности; приемы структурирования информации; - формат оформления результатов поиска информации - содержание актуальной нормативно-правовой документации;	Уровень правильных ответов при письменном и устном контроле, четкость изложения материала. Быстрота ориентации в представляемом материале, быстрота реакции на вопросы. Правильность, полнота выполнения заданий, точность формулировок, точность расчетов, соответствие требованиям.	устный опрос, практические работы

- современная научная и профессиональная терминология; - возможные траектории профессионального развития и самообразования - психологические основы деятельности коллектива, - психологические особенности личности; - основы проектной деятельности - особенности социального и культурного контекста; - правила оформления документов и построения устных сообщений - назначение, состав, основные характеристики организационной и компьютерной техники;		
- основные компоненты информационных систем, принципы внедрения информационных систем, организацию межсетевого взаимодействия; - назначение и принципы использования системного и прикладного программного обеспечения; - принципы защиты информации от несанкционированного доступа; - правовые аспекты использования информационных технологий и программного обеспечения; - основные понятия	Оптимальность выбора способов действий, методов, последовательностей действий. Соответствие требованиям инструкций, регламентов, рациональность действий. Точность распознавания проблемных ситуаций в различных контекстах; Адекватность анализа сложных ситуаций при решении задач профессиональной деятельности, эффективность поиска. Точность определения источников нужных ресурсов. Разработка детального плана действий, правильность оценки рисков на каждом шагу; Точность оценки плюсов и минусов полученного результата, своего плана и его реализации, предложение критериев оценки и рекомендаций по улучшению плана	Текущий контроль: экспертное наблюдение и оценка в процессе выполнения заданий для практических занятий;

автоматизированной обработки информации;		
---	--	--

Для оценки достижения запланированных результатов обучения по дисциплине разработаны контрольно-оценочные средства для проведения текущего контроля и промежуточной аттестации, которые прилагаются к рабочей программе дисциплины.

Для оценки достижения запланированных результатов обучения по дисциплине разработаны контрольно-оценочные средства для проведения текущего контроля и промежуточной аттестации, которые прилагаются к рабочей программе дисциплины.

Оценка результатов обучения производится при помощи бально-рейтинговой системы.

Основные критерии оценки:

- конспектирование 0,5 баллов;
- активность на уроке 0,5 баллов;
- посещаемость занятий 0,5 баллов;
- выполнение индивидуальных домашних заданий 1 задание- 1 балл;
- выполнение самостоятельной работы 1 балл;
- лабораторная работа 3 балла;
- контрольная работа 1 задание -1 балл;
- участие в научно-исследовательской работе 15 баллов;
- дифференцированный зачет 20 баллов.

МИНОБРНАУКИ РОССИИ
ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля и промежуточной аттестации
по учебной дисциплине

*МДК.06.02 Инженерно-техническая поддержка сопровождения
информационных систем*
программы подготовки специалистов среднего звена /
квалифицированных рабочих и служащих

09.02.07 Информационные системы и программирование

Форма обучения: очная

Оценочные средства для проведения текущего контроля и промежуточной аттестации по учебной дисциплине *МДК.06.02 Инженерно-техническая поддержка сопровождения информационных систем* разработаны в соответствии с требованиями ФГОС СПО по специальности / профессии *09.02.07 Информационные системы и программирование*, утвержденного приказом Минобрнауки России от «09» декабря 2016 г. № 1547, примерной образовательной программой.

Разработчик(и): *Лихацкий М.Б. преподаватель ОСПО филиала ФГБОУ ВО «ВВГУ» в г. Находке*

Рассмотрено и одобрено на заседании цикловой методической комиссии

Протокол № 10 от «29» июня 2026 г.

Председатель ЦМК _____ *В.В Плахотина*
подпись

1 Общие сведения

Фонд оценочных средств (далее – ФОС) предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины *МДК.06.02 Инженерно-техническая поддержка сопровождения информационных систем*

ФОС включают в себя контрольные материалы для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине, которая проводится в форме дифференцированного зачёта (с использованием оценочного средства - *тестирование*)

2 Планируемые результаты обучения по дисциплине, обеспечивающие результаты освоения образовательной программы

Код ОК, ПК	Код результата обучения	Наименование результата обучения ¹
ОК 1 ОК 2	31	Назначение и виды сопровождения ИС, технологии резервного копирования и восстановления данных.
ОК 4 ОК 5	32	Состав, структуру, принципы реализации и функционирования систем резервного копирования и мониторинга.
ОК 9 ОК 10	33	Базовые и прикладные технологии администрирования и безопасности ИС.
ПК 5.1 ПК 5.2	34	Инструментальные средства для диагностики, мониторинга и администрирования ИС
ПК 5.6 ПК 6.3	У1	Выполнять резервное копирование и восстановление данных ИС.
	У2	Проводить мониторинг и диагностику работоспособности ИС.
	У3	Обеспечивать безопасность функционирования ИС

3 Соответствие оценочных средств контролируемым результатам обучения

Краткое наименование раздела (модуля) / темы дисциплины	Код результата обучения	Показатель ² овладения результатами обучения	Наименование оценочного средства и представление его в КОС	
			Текущий контроль	Промежуточная аттестация
Тема 1.1 Организация сопровождения и восстановления работоспособности системы	31	Способность понимать назначение и виды резервного копирования, политики восстановления	<i>Устный опрос (п 5.1 вопросы 1-5) Практическая работа №1-2 (п 5.2)</i>	<i>Устный опрос (п 6.1 вопросы 1-18) Тест вариант №1-2 (п 6.2)</i>
	32	Способность описать структуру и принципы функционирования систем резервного копирования		
	У1	Способность выполнять резервное копирование и восстановление данных		
Тема 1.2. Администрирование и безопасность информационной системы	33	Способность применять технологии администрирования и безопасности	<i>Устный опрос (п 5.1 вопросы 6-10) Практическая работа №3-5 (п 5.2)</i>	<i>Устный опрос (п 6.1 вопросы 1-18) Тест вариант №1-2 (п 6.2)</i>
	34	Способность использовать инструментальные средства для администрирования		
	У3	Способность настраивать права доступа и устанавливать обновления		
Тема 1.3 Идентификация и устранение ошибок в информационной системе	У2	Способность проводить мониторинг и диагностику	<i>Устный опрос (п 5.1 вопросы 11-18) Практическая работа №6-8 (п 5.2)</i>	<i>Устный опрос (п 6.1 вопросы 1-18) Тест вариант №1-2 (п 6.2)</i>
	У4	Способность анализировать логи и составлять отчёты об ошибках		
	У1	Способность выполнять резервное копирование и восстановление данных		

4. Описание процедуры оценивания

Результаты обучения по дисциплине, уровень сформированности компетенций оцениваются по четырёх бальной шкале оценками: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Текущая аттестация по дисциплине проводится с целью систематической проверки достижений обучающихся. Объектами оценивания являются: степень усвоения теоретических знаний, уровень овладения практическими умениями и навыками по всем видам учебной работы, качество выполнения самостоятельной работы, учебная дисциплина (активность на занятиях, своевременность выполнения различных видов заданий, посещаемость всех видов занятий по аттестуемой дисциплине).

При проведении промежуточной аттестации оценивается достижение студентом запланированных по дисциплине результатов обучения, обеспечивающих результаты освоения образовательной программы в целом. *Оценка на зачете выставляется с учетом оценок, полученных при прохождении текущей аттестации.*

Критерии оценивания устного ответа

(оценочные средства: *собеседование, устное сообщение*)

5 баллов - ответ показывает прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа; умение приводить примеры современных проблем изучаемой области.

4 балла - ответ, обнаруживающий прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа. Однако допускается одна - две неточности в ответе.

3 балла – ответ, свидетельствующий в основном о знании процессов изучаемой предметной области, отличающийся недостаточной глубиной и полнотой раскрытия темы; знанием основных вопросов теории; слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры; недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается несколько ошибок в содержании ответа; неумение привести пример развития ситуации, провести связь с другими аспектами изучаемой области.

2 балла – ответ, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы; незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов; неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Допускаются серьезные ошибки в содержании ответа; незнание современной проблематики изучаемой области.

Критерии оценивания письменной работы

(оценочные средства: *реферат, конспект, контрольная работа, расчетно-графическая работа, доклад (сообщение), в том числе выполненный в форме презентации, творческое задание*).

5 баллов - студент выразил своё мнение по сформулированной проблеме, аргументировал его, точно определив ее содержание и составляющие. Проблема раскрыта полностью, выводы обоснованы. Приведены данные отечественной и зарубежной литературы, статистические сведения, информация нормативно-правового характера. Студент владеет навыком самостоятельной работы по заданной теме; методами и приемами анализа теоретических и/или практических аспектов изучаемой области. Фактических ошибок, связанных с пониманием проблемы, нет; графически работа оформлена правильно.

4 балла - работа характеризуется смысловой цельностью, связностью и последовательностью изложения; допущено не более 1 ошибки при объяснении смысла или содержания проблемы. Проблема раскрыта. Не все выводы сделаны и/или обоснованы. Для аргументации приводятся данные отечественных и зарубежных авторов. Продемонстрированы исследовательские умения и навыки. Фактических ошибок, связанных с пониманием проблемы, нет. Допущены одна-две ошибки в оформлении работы.

3 балла – студент проводит достаточно самостоятельный анализ основных этапов и смысловых составляющих проблемы; понимает базовые основы и теоретическое обоснование выбранной темы. Проблема раскрыта не полностью. Выводы не сделаны и/или выводы не обоснованы. Проведен анализ проблемы без привлечения дополнительной литературы. Допущено не более 2 ошибок в смысле или содержании проблемы, оформлении работы.

2 балла - работа представляет собой пересказанный или полностью переписанный исходный текст без каких бы то ни было комментариев, анализа. Не раскрыта структура и теоретическая составляющая темы. Проблема не раскрыта. Выводы отсутствуют. Допущено три или более трех ошибок в смысловом содержании раскрываемой проблемы, в оформлении работы.

Критерии оценивания тестового задания

Оценка	Отлично	Хорошо	Удовлетворительно	Неудовлетворительно
Количество правильных ответов	91 % и $\geq$	от 81% до 90,9 %	не менее 70%	менее 70%

Критерии выставления оценки студенту на зачете

(оценочные средства: устный опрос в форме ответов на вопросы билетов, устный опрос в форме собеседования, выполнение письменных разноуровневых задач и заданий, комплексная расчетно-графическая работа, творческое задание, кейс-задача, портфолио, проект и т.п.)

Оценка по промежуточной аттестации	Характеристика качества сформированности компетенций
«зачтено» / «отлично»	Студент демонстрирует сформированность дисциплинарных компетенций на продвинутом уровне: обнаруживает всестороннее, систематическое и глубокое знание учебного материала, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач.
«зачтено» / «хорошо»	Студент демонстрирует сформированность дисциплинарных компетенций на базовом уровне: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
«зачтено» / «удовлетворительно»	Студент демонстрирует сформированность дисциплинарных компетенций на пороговом уровне: имеет знания только основного материала, но не усвоил его деталей, в ходе контрольных мероприятий допускаются значительные ошибки, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного

	материала, испытывает затруднения при выполнении практических работ, при оперировании знаниями и умениями при их переносе на новые ситуации.
«не зачтено» / «неудовлетворительно»	Студент демонстрирует сформированность дисциплинарных компетенций на уровне ниже порогового: выявляется полное или практически полное отсутствие знаний значительной части программного материала, студент допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы, умения и навыки не сформированы.

5. Примеры оценочных средств для проведения текущей аттестации

5.1 Вопросы для устного опроса

1. Дайте определение сопровождения информационной системы. Каковы его основные цели?
2. Что такое инцидент в IT? Чем он отличается от проблемы?
3. Опишите основные этапы обработки инцидента.
4. Что такое Соглашение об уровне обслуживания (SLA) и какую роль оно играет?
5. Что такое резервное копирование и каковы его основные цели?
6. В чём разница между полным, инкрементным и дифференциальным резервным копированием?
7. Объясните разницу между целевым временем восстановления (RTO) и целевой точкой восстановления (RPO).
8. Что такое план аварийного восстановления и какие ключевые элементы он должен включать?
9. Для чего используются контрольные точки восстановления в операционных системах?
10. Что такое отказоустойчивый кластер и как он повышает доступность системы?
11. Перечислите основные обязанности системного администратора.
12. Что подразумевается под информационной безопасностью? Назовите три её ключевых аспекта (CIA-триада).
13. Объясните разницу между аутентификацией и авторизацией.
14. Что такое политика паролей и какие современные требования к ним предъявляются?
15. Что такое многофакторная аутентификация и почему она эффективнее однофакторной?
16. Каковы основные задачи межсетевого экрана (брандмауэра)?
17. Что такое система обнаружения и предотвращения вторжений?
18. Для чего необходима установка патчей и обновлений безопасности?

5.2 Примеры практических работ

ПРАКТИЧЕСКАЯ РАБОТА №1

Тема: Разработка плана резервного копирования

Цель:

Научиться разрабатывать стратегию резервного копирования для информационной системы с учётом требований RTO и RPO, определять типы бэкапов и регламент.

Задание:

Для заданной информационной системы (например, файловый сервер, база данных 1С, веб-приложение) разработать план резервного копирования, включающий:

- перечень данных для копирования;

- выбор типа резервного копирования (полное, инкрементное, дифференциальное);
- частоту и расписание;
- выбор носителя и места хранения (локальное, облачное, off-site);
- процедуру проверки целостности копий;
- порядок восстановления (с указанием RTO и RPO).

Порядок выполнения:

1. Ознакомиться с архитектурой заданной ИС (описание выдаётся преподавателем).
2. Определить критичные данные (базы данных, файлы конфигурации, журналы).
3. Рассчитать приблизительный объём данных и требуемое место для хранения.
4. Выбрать типы копирования:
 - полное – например, еженедельно;
 - дифференциальное – ежедневно;
 - инкрементное – каждый час (если требуется).
5. Составить график: день недели, время, тип.
6. Определить способ хранения: сетевой диск, ленточная библиотека, облачный сервис.
7. Описать процедуру проверки копий (тестовое восстановление на отдельном сервере).
8. Оформить план в виде документа (таблицы, схемы).
9. Сдать отчёт преподавателю.

Содержание отчёта:

- Название ИС, состав данных.
- Обоснование выбранных типов копирования и расписания.
- Таблица с расписанием.
- Описание хранилища и политики хранения (сроки хранения).
- Инструкция по проверке целостности.
- Критерии успешности (RTO, RPO).

Контрольные вопросы:

1. Чем отличается инкрементное копирование от дифференциального?
2. Как влияет RPO на частоту бэкапов?
3. Почему важно хранить копии вне офиса (off-site)?
4. Какие риски существуют при использовании только одного типа копирования?

ПРАКТИЧЕСКАЯ РАБОТА №2

Тема: Создание резервной копии информационной системы

Цель:

Получить практические навыки создания резервных копий файлов, системного состояния и баз данных с использованием штатных средств ОС.

Задание:

Выполнить резервное копирование:

- папки с документами (например, C:\Data);
- системного состояния (реестр, загрузочные файлы) с помощью wbadmin;
- базы данных (например, SQL Server Express или просто копирование файлов .mdf).

Использовать разные типы: полное и инкрементное (через архиватор или командные утилиты).

Порядок выполнения:

1. Создать тестовую папку с файлами (или использовать существующую).
2. Создать полную копию папки с помощью robocopy или архиватора (7-Zip).
3. Изменить несколько файлов (добавить, отредактировать).
4. Создать инкрементную копию (только изменённые файлы) – можно использовать robocopy /MIR или архиватор с параметром.
5. Создать резервную копию системного состояния командой:
wbadmin start backup -backupTarget:E: -include:C: -systemState (подставить свой диск).
6. Для БД – если есть SQL Server, выполнить команду BACKUP DATABASE ... TO DISK; если нет

– просто скопировать файлы базы данных (при остановленной службе).

7. Проверить созданные копии на целостность.
8. Составить отчёт с командами и скриншотами результатов.

Содержание отчёта:

- Перечень использованных инструментов.
- Скриншоты процесса и результатов.
- Команды, которые применялись.
- Сравнение размера полной и инкрементной копий.
- Выводы о времени выполнения.

Контрольные вопросы:

1. Какие утилиты Windows позволяют создавать бэкапы?
2. В чём преимущество wbadmin перед простым копированием?
3. Как проверить, что резервная копия создана корректно?
4. Почему для баз данных лучше использовать специальные утилиты, а не простое копирование?

ПРАКТИЧЕСКАЯ РАБОТА №3

Тема: Восстановление данных

Цель:

Освоить методы восстановления файлов и данных из резервных копий, используя различные инструменты.

Задание:

1. Смоделировать ситуацию потери данных (удалить несколько файлов из папки).
2. Восстановить файлы из полной и инкрементной копий.
3. Восстановить системное состояние из бэкапа (на виртуальной машине).
4. Восстановить базу данных из бэкапа (если есть SQL Server).

Порядок выполнения:

1. Удалить тестовые файлы или папку.
2. Восстановить файлы, скопировав их из бэкапа (например, из архива или через robocopy).
3. Для системного состояния: запустить wbadmin start recovery и восстановить состояние (потребуется перезагрузка).
4. Для БД: выполнить RESTORE DATABASE ... FROM DISK.
5. Проверить, что данные восстановлены и работоспособны.
6. Сделать скриншоты процесса и результата.

Содержание отчёта:

- Описание сценария потери данных.
- Команды восстановления.
- Скриншоты до и после.
- Время, затраченное на восстановление.
- Сравнение с теоретическим RTO.

Контрольные вопросы:

1. В чём сложность восстановления из инкрементных копий?
2. Что делать, если резервная копия повреждена?
3. Как восстановить систему, если она не загружается?
4. Какие существуют альтернативные методы восстановления?

ПРАКТИЧЕСКАЯ РАБОТА №4

Тема: Восстановление работоспособности системы

Цель:

Научиться восстанавливать операционную систему после критических сбоев с использованием точек восстановления, образов и загрузочных носителей.

Задание:

1. Создать точку восстановления системы.
2. Установить заведомо проблемное обновление или драйвер (или симулировать сбой).
3. Выполнить откат системы к точке восстановления.
4. Создать образ системы (средствами Windows) и восстановить его на тестовой машине.
5. Подготовить загрузочный диск восстановления и протестировать загрузку в режиме восстановления.

Порядок выполнения:

1. Создать точку восстановления (вручную через интерфейс или PowerShell).
2. Установить драйвер, который может вызвать проблемы (или использовать утилиту для симуляции сбоя).
3. Перезагрузить и убедиться в неработоспособности.
4. Загрузиться в безопасном режиме и выполнить откат к точке.
5. Создать полный образ системы с помощью wadmin или «Архивация и восстановление».
6. Восстановить образ на другой виртуальной машине (или на раздел).
7. Записать загрузочный диск восстановления (создать USB-носитель) и проверить его работу.

Содержание отчёта:

- Описание каждого шага с командами и скриншотами.
- Сравнение времени восстановления через точки и через образ.
- Анализ плюсов и минусов каждого метода.

Контрольные вопросы:

1. Чем точка восстановления отличается от образа системы?
2. Какие данные сохраняет точка восстановления?
3. Что такое «восстановление при загрузке» (Startup Repair)?
4. Как часто следует создавать образы системы?

ПРАКТИЧЕСКАЯ РАБОТА №5

Тема: Создание резервной копии базы данных

Цель:

Освоить методы резервного копирования баз данных (на примере SQL Server или любой доступной СУБД) и научиться настраивать автоматическое резервирование.

Задание:

1. Установить (или использовать имеющуюся) СУБД (например, SQL Server Express или PostgreSQL).
2. Создать тестовую базу данных и заполнить её данными.
3. Выполнить полное резервное копирование базы данных через интерфейс и через T-SQL.
4. Выполнить дифференциальное или инкрементное копирование (если поддерживается).
5. Настроить автоматическое выполнение бэкапа по расписанию (используя SQL Agent или планировщик Windows).
6. Проверить возможность восстановления из созданных копий.

Порядок выполнения:

1. Создать БД, таблицу, вставить несколько записей.
2. Через SSMS (или pgAdmin) выполнить резервное копирование (задать путь, тип).
3. Записать команду T-SQL:

sql

```
BACKUP DATABASE TestDB TO DISK = 'C:\Backup\TestDB_full.bak';
```

4. Внести изменения (добавить строки).
5. Выполнить дифференциальный бэкап:

sql

```
BACKUP DATABASE TestDB TO DISK = 'C:\Backup\TestDB_diff.bak' WITH DIFFERENTIAL;
```

6. Настроить задание в планировщике Windows для выполнения команд каждые 12 часов.
7. Удалить базу и восстановить её из полного и дифференциального бэкапов.

8. Проверить целостность данных.

Содержание отчёта:

- Схема БД.
- SQL-команды для бэкапа и восстановления.
- Настройки расписания (скриншоты).
- Отчёт о восстановлении (количество записей).
- Оценка времени выполнения.

Контрольные вопросы:

1. В чём отличие резервного копирования БД от копирования файлов .mdf?
2. Что такое журнал транзакций и как его бэкапить?
3. Как восстановить БД до конкретного момента времени?
4. Какие существуют модели восстановления (Simple, Full, Bulk-Logged)?

ПРАКТИЧЕСКАЯ РАБОТА №6

Тема: Сбор информации об ошибках. Формирование отчетов об ошибках

Цель:

Научиться собирать диагностическую информацию об ошибках с использованием системных журналов, мониторинга и утилит, а также оформлять отчёт об ошибке по установленному шаблону.

Задание:

1. Смоделировать ошибку в приложении или системе (например, вызвать сбой службы или ошибку приложения).
2. Собрать данные:
 - системный журнал (Event Viewer);
 - журнал приложения;
 - журнал безопасности (если есть);
 - параметры производительности (Task Manager, Performance Monitor);
 - дамп памяти (если требуется).
3. Проанализировать собранную информацию, выявить возможную причину.
4. Оформить официальный отчёт об ошибке с использованием типового шаблона (см. приложение).
5. Предложить рекомендации по устранению.

Порядок выполнения:

1. Создать ошибку: например, запустить скрипт, который вызывает деление на ноль в простой программе, или остановить службу, или использовать утилиту для краша.
2. Открыть «Просмотр событий» -> «Журнал Windows» -> «Приложение» и «Система», найти соответствующие ошибки (код события, источник).
3. Сохранить события в файлы (Export).
4. Запустить монитор производительности и зафиксировать нагрузку в момент ошибки.
5. Если есть дамп памяти – сохранить.
6. Заполнить отчёт по форме:
 - Дата и время инцидента;
 - Описание симптомов;
 - Результаты сбора логов;
 - Предварительный анализ;
 - Рекомендации.
7. Предоставить отчёт в печатном виде.

Содержание отчёта:

- Титульный лист.
- Журнал событий с выделением ошибок.
- Скриншоты мониторинга.
- Таблица с анализом.

- Выводы и рекомендации.

Контрольные вопросы:

1. Какие уровни событий бывают в Event Viewer (Information, Warning, Error, Critical)?
2. Как настроить подробное журналирование для приложения?
3. Что такое ID события и как он помогает в поиске решения?
4. Какие ещё источники информации об ошибках существуют (логи IIS, SQL Server, etc.)?

Шаблон отчёта об ошибке (для работы №6)

Можно приложить к методическим указаниям:

ОТЧЁТ ОБ ОШИБКЕ № ____

1. Дата и время обнаружения:
2. Заявитель (кто сообщил):
3. Симптомы (краткое описание):
4. Окружение (ОС, версия ПО):
5. Действия, приводящие к ошибке:
6. Диагностическая информация (приложить логи, скриншоты):
 - Журнал событий:
 - Метрики производительности:
 - Файлы дампа:
7. Анализ вероятных причин:
8. Предварительные рекомендации по устранению:
9. Исполнитель:
10. Дата заполнения:

ПРАКТИЧЕСКАЯ РАБОТА №7

Тема: Выявление и устранение ошибок программного кода информационных систем

Цель:

Получить навыки поиска и исправления ошибок в программном коде (на примере скриптов, C#, или другого языка) с использованием отладчика и статического анализа.

Задание:

1. Получить от преподавателя исходный код (программа на C#, Python или скрипт) с несколькими ошибками: логическими, синтаксическими, связанными с работой с файлами или БД.
2. Выполнить статический анализ кода (визуально или с помощью IDE).
3. Запустить отладку (пошагово) и найти места сбоев.
4. Исправить ошибки, повторно протестировать.
5. Оформить отчёт: описание каждой ошибки, способ обнаружения, исправление, результат тестирования.

Порядок выполнения:

1. Получить архив с проектом.
2. Открыть проект в среде разработки (Visual Studio, PyCharm и т.п.).
3. Запустить приложение – выявить ошибки (зависания, исключения, неверные результаты).
4. Использовать отладчик: установить точки останова, просмотреть значения переменных.
5. Исправить код:
 - синтаксические ошибки – исправить синтаксис;
 - логические ошибки – изменить условие, добавить проверки;
 - ошибки ввода-вывода – добавить обработку исключений.
6. Повторно выполнить программу с разными входными данными, чтобы убедиться в корректности.
7. Зафиксировать изменения в отчёте.

Содержание отчёта:

- Исходный код с выделением ошибок (можно до и после).
- Описание каждой ошибки и её исправления.
- Скриншоты процесса отладки.
- Результаты тестирования после исправления.
- Выводы.

Контрольные вопросы:

1. Какие инструменты отладки вы использовали?
2. Чем отличается исключение (exception) от ошибки компиляции?
3. Как проверить работу программы на граничных значениях?
4. Как обрабатывать ошибки при работе с БД?

ПРАКТИЧЕСКАЯ РАБОТА №8

Тема: Выполнение обслуживания информационной системы в соответствии с пользовательской документацией

Цель:

Научиться выполнять регламентные процедуры обслуживания ИС, опираясь на руководство администратора и пользователя, и фиксировать результаты.

Задание:

1. Получить фрагмент руководства администратора для некоторой ИС (например, конфигурация сервера, обновление, очистка логов).
2. Выполнить перечень операций в соответствии с регламентом (в учебной лаборатории):
 - Проверка статуса служб;
 - Очистка временных файлов и логов;
 - Проверка свободного места;
 - Проверка резервных копий;
 - Проверка работоспособности через тестовые сценарии.
3. Заполнить журнал обслуживания с датой, действием и результатом.
4. Сделать выводы о состоянии системы.

Порядок выполнения:

1. Изучить предоставленную документацию (инструкция по обслуживанию).
2. Создать контрольный лист операций.
3. Поочерёдно выполнить операции в системе:
 - открыть службы (services.msc), убедиться, что все критичные запущены;
 - очистить папку C:\Windows\Temp и логи (eventvwr – очистка старых событий);
 - проверить свободное место на диске;
 - проверить целостность бэкапов (последние даты).
4. Выполнить тестовые сценарии (например, загрузить интерфейс, создать документ).
5. Записать все результаты в журнал (можно создать таблицу Excel).
6. Подготовить краткое заключение.

Содержание отчёта:

- Титульный лист.
- Изученный документ (его реквизиты).
- Журнал обслуживания (таблица: дата, действие, ожидаемый результат, фактический результат, примечание).
- Вывод о работоспособности системы.
- Рекомендации.

Контрольные вопросы:

1. Почему важно следовать задокументированной процедуре, а не действовать по своему усмотрению?
2. Какие риски могут возникнуть при очистке логов?
3. Как часто нужно проводить регламентное обслуживание?

4. Что делать, если фактические результаты отличаются от ожидаемых?
-

6. Оценочные средства для проведения промежуточной аттестации

6.1 Вопросы для собеседования при проведении дифференцированного зачета

1. Дайте определение сопровождения информационной системы. Перечислите основные задачи сопровождения.
2. Какие виды резервного копирования вы знаете? Опишите их достоинства и недостатки.
3. Что такое SLA, RTO и RPO? Как эти показатели связаны с планированием восстановления?
4. Опишите структуру плана аварийного восстановления (Disaster Recovery Plan).
5. Каковы основные обязанности системного администратора в процессе сопровождения ИС?
6. Что такое инцидент и какова процедура его обработки? Чем инцидент отличается от проблемы?
7. Опишите процесс управления изменениями в ИС. Почему он важен?
8. Какие методы обеспечения безопасности информационной системы вы знаете?
9. Что такое аутентификация, авторизация и аудит? Приведите примеры.
10. Какие существуют виды вредоносного ПО и как от них защищаться?
11. Что такое межсетевой экран (брандмауэр) и каковы его функции?
12. Опишите процесс диагностики и устранения ошибок в ИС. Какие инструменты используются?
13. Что такое журналы событий (логи) и как они помогают в поиске ошибок?
14. Какие встроенные утилиты Windows вы знаете для мониторинга и диагностики?
15. Как определить, что причина сбоя – аппаратная, а не программная?
16. Что такое "синий экран смерти" и как анализировать его причины?
17. Опишите алгоритм действий при потере сетевого подключения у пользователя.
18. Почему важно документировать все действия по устранению ошибок?

6.2 Тестовые материалы

Вариант №1

Часть 1. Выбор одного правильного ответа (вопросы 1–3)

1. **Что из перечисленного является целью резервного копирования?**
 - А) Увеличение производительности системы
 - Б) Обеспечение возможности восстановления данных после сбоя
 - В) Ускорение работы приложений
 - Г) Сокращение объема хранимых данных
2. **Какой тип резервного копирования занимает меньше всего места для хранения?**
 - А) Полное
 - Б) Инкрементное
 - В) Дифференциальное
 - Г) Зеркальное
3. **Что такое SLA в контексте сопровождения ИС?**
 - А) Соглашение об уровне обслуживания
 - Б) План аварийного восстановления
 - В) Протокол сетевого взаимодействия
 - Г) Система управления базами данных

Часть 2. Установление соответствия (вопросы 4–6)

4. Установите соответствие между термином и его определением.

Термин	Определение
1. RTO	А. Максимально допустимый объём потери данных
2. RPO	Б. Максимально допустимое время восстановления системы
3. Инцидент	В. Событие, нарушающее нормальную работу услуги

Ответ запишите в виде сочетания цифр и букв (например, 1-Б, 2-А, 3-В).

5. Установите соответствие между типом резервного копирования и его характеристикой.

Тип	Характеристика
1. Полное	А. Копируются только изменения с момента последнего бэкапа любого типа
2. Инкрементное	Б. Копируются все данные, занимает много места, восстановление быстрое
3. Дифференциальное	В. Копируются изменения с момента последнего полного бэкапа

6. Установите соответствие между действием администратора и областью безопасности.

Действие	Область безопасности
1. Назначение паролей и прав доступа	А. Защита от вредоносного ПО
2. Установка обновлений безопасности	Б. Управление доступом (аутентификация и авторизация)
3. Настройка антивируса	В. Устранение уязвимостей (патчинг)

Часть 3. Установление последовательности (вопросы 7–9)

7. Установите правильную последовательность этапов обработки инцидента:

1. Закрытие инцидента
2. Регистрация
3. Диагностика
4. Решение (восстановление)
5. Классификация

8. Расставьте в правильном порядке шаги по восстановлению системы из резервной копии:

1. Загрузка с загрузочного носителя
2. Запуск процесса восстановления
3. Выбор точки восстановления (даты)
4. Проверка целостности восстановленных данных
5. Перезагрузка и тестирование работоспособности

9. Установите последовательность действий при диагностике сетевой неисправности:

1. Проверка физического подключения (кабель, Wi-Fi)
2. Проверка IP-настроек (команда ipconfig)
3. Проверка доступности шлюза (команда ping)
4. Проверка DNS-резолвинга (команда nslookup)
5. Проверка маршрута до удалённого сервера (команда tracert)

Часть 4. Открытые вопросы (вопросы 10–12)

10. Опишите разницу между полным, инкрементным и дифференциальным резервным копированием. В каких ситуациях каждый из них предпочтительнее?
11. Что такое «план аварийного восстановления» (Disaster Recovery Plan)? Какие обязательные разделы он должен содержать?
12. Опишите алгоритм действий системного администратора при обнаружении подозрительной активности (взлома или вируса) на сервере.

Вариант №2

Часть 1. Выбор одного правильного ответа (вопросы 1–3)

1. **Что такое инкрементное резервное копирование?**
 - А) Копирование всех данных каждый раз
 - Б) Копирование только изменений с момента последнего бэкапа (любого типа)
 - В) Копирование изменений с момента последнего полного бэкапа
 - Г) Копирование данных на внешний носитель в реальном времени
2. **Какой процесс управляет изменениями в ИС для минимизации рисков?**
 - А) Управление инцидентами
 - Б) Управление изменениями
 - В) Управление проблемами
 - Г) Управление доступом
3. **Что такое «проблема» в терминологии ITIL?**
 - А) Одиночный инцидент
 - Б) Причина одного или нескольких инцидентов
 - В) Жалоба пользователя
 - Г) Запрос на новый функционал

Часть 2. Установление соответствия (вопросы 4–6)

4. Установите соответствие между компонентом системы мониторинга и его функцией.

Компонент	Функция
1. Система журналирования (логи)	А. Оповещение администратора о критических событиях
2. Система алертинга (оповещений)	Б. Запись всех событий и ошибок работы системы
3. Система сбора метрик (Zabbix, Prometheus)	В. Сбор и визуализация показателей производительности

5. Установите соответствие между методом обеспечения безопасности и его описанием.

Метод	Описание
1. Аутентификация	А. Определение разрешённых действий пользователя
2. Авторизация	Б. Проверка подлинности пользователя (кто ты)
3. Аудит	В. Запись действий пользователя для последующего анализа

6. Установите соответствие между этапом жизненного цикла ИС и выполняемой на нём задачей сопровождения.

Этап ЖЦ	Задача сопровождения
1. Эксплуатация	А. Обновление версий ПО, установка патчей
2. Сопровождение и развитие	Б. Мониторинг работоспособности, решение инцидентов
3. Вывод из эксплуатации	В. Миграция данных в новую систему, архивация

Часть 3. Установление последовательности (вопросы 7–9)

7. **Установите правильную последовательность действий при внедрении нового обновления безопасности:**
 1. Тестирование обновления на тестовом стенде
 2. Создание контрольной точки восстановления (бэкап)
 3. Установка обновления на продуктивных серверах
 4. Мониторинг стабильности работы системы после установки
 5. Документирование результатов установки
8. **Расставьте шаги по созданию резервной копии базы данных:**
 1. Остановка служб, использующих БД (если требуется)
 2. Выбор типа копирования (полное/инкрементное)
 3. Запуск процесса резервного копирования
 4. Проверка целостности созданной копии
 5. Перемещение копии на внешнее хранилище (off-site)

9. Установите последовательность этапов диагностики проблемы, о которой сообщил пользователь:

1. Воспроизведение проблемы на рабочем месте пользователя
2. Опрос пользователя (сбор симптомов)
3. Анализ системных журналов и метрик
4. Формулировка гипотезы о причине
5. Проверка гипотезы и устранение неисправности

Часть 4. Открытые вопросы (вопросы 10–12)

10. Объясните разницу между управлением инцидентами и управлением проблемами. Приведите по одному примеру.
 11. Какие основные утилиты операционной системы Windows вы используете для мониторинга и диагностики? Назовите минимум 5 и кратко опишите их назначение.
 12. Опишите, как вы будете действовать, если пользователь сообщает, что «не может зайти в систему» (ввод логина и пароля не работает). Перечислите пошаговый алгоритм диагностики.
-

6.3 Ключи к тестовым заданиям для проведения промежуточной аттестации

Вариант №1

Часть 1 (выбор):

1 – Б, 2 – Б, 3 – А

Часть 2 (соответствие):

4 – 1-Б, 2-А, 3-В

5 – 1-Б, 2-А, 3-В (примечание: для инкрементного – А, для дифференциального – В)

6 – 1-Б, 2-В, 3-А

Часть 3 (последовательность):

7 – 2, 5, 3, 4, 1 (регистрация → классификация → диагностика → решение → закрытие)

8 – 1, 3, 2, 4, 5 (загрузка → выбор точки → запуск восстановления → проверка → перезагрузка)

9 – 1, 2, 3, 5, 4 (физика → ipconfig → ping → tracert → nslookup)

Вариант №2

Часть 1 (выбор):

1 – Б, 2 – Б, 3 – Б

Часть 2 (соответствие):

4 – 1-Б, 2-А, 3-В

5 – 1-Б, 2-А, 3-В

6 – 1-Б, 2-А, 3-В

Часть 3 (последовательность):

7 – 2, 1, 3, 4, 5 (бэкап → тест → установка → мониторинг → документирование)

8 – 2, 1, 3, 4, 5 (выбор типа → остановка служб → запуск → проверка → вынос на внешнее хранилище)

9 – 2, 1, 3, 4, 5 (опрос → воспроизведение → анализ логов → гипотеза → проверка)

Вариант №1

10.

- Полное – копируются все данные. Занимает много места, но восстановление самое быстрое. Используется при небольшом объёме данных или в начале недели/месяца.
- Инкрементное – копируются только изменения с момента последнего бэкапа (любого типа). Экономит место, но восстановление требует последовательного применения всех инкрементов.

Используется при частых бэкапах (ежедневно).

- Дифференциальное – копируются изменения с момента последнего полного бэкапа. Компромисс: быстрее восстановления, чем инкрементное, но занимает больше места. Используется, если нужен баланс между скоростью восстановления и объёмом хранилища.

11.

План аварийного восстановления (DRP) – это документированный набор процедур для восстановления ИТ-инфраструктуры после крупных сбоев (пожар, наводнение, кибератака).

Обязательные разделы:

- Цели восстановления (RTO и RPO)
- Список критических систем и их приоритет
- Схема коммуникации (кто кого оповещает)
- Порядок действий по восстановлению (пошагово)
- Роли и ответственность членов команды
- План тестирования DRP (периодические учения)

12.

Алгоритм при подозрении на взлом/вирус:

1. Изолировать заражённый сервер от сети (отключить сетевой кабель или отключить порт на свитче).
2. Оповестить руководство и службу безопасности.
3. Сохранить логи и образ памяти для анализа (криминалистика).
4. Запустить полное антивирусное сканирование.
5. Если обнаружен вирус – попытаться вылечить; если не удаётся – переустановить систему из заведомо чистого образа.
6. Восстановить данные из резервных копий (предварительно проверив их на чистоту).
7. Провести аудит уязвимостей и закрыть найденные дыры.
8. Сменить все пароли доступа.
9. Задokumentировать инцидент и принятые меры.

Вариант №2

10.

- Управление инцидентами – фокусируется на быстром восстановлении работоспособности, предоставлении временного решения (workaround). Пример: пользователь не может войти – администратор сбрасывает пароль и разблокирует учётную запись.
- Управление проблемами – направлено на поиск корневой причины и её устранение, чтобы инциденты не повторялись. Пример: аналитик выясняет, что пароли сбрасываются из-за политики автоматического блокирования при превышении времени ожидания, и изменяет эту политику.

11.

Минимум 5 утилит Windows:

- ping – проверка доступности сетевого узла
- ipconfig – просмотр и обновление IP-конфигурации
- netstat – просмотр активных сетевых подключений и прослушиваемых портов
- Task Manager (Диспетчер задач) – просмотр запущенных процессов, загрузки CPU/памяти/диска
- Event Viewer (Просмотр событий) – просмотр системных, прикладных и безопасностных логов
- chkdsk – проверка целостности файловой системы и исправление ошибок диска
- sfc – проверка и восстановление системных файлов

12.

Алгоритм при проблеме входа:

1. Уточнить у пользователя: какое сообщение об ошибке, правильный ли логин, не менял ли он пароль.
2. Проверить раскладку клавиатуры и Caps Lock.

3. Проверить сетевой доступ (если учётная запись доменная) – пингуется ли контроллер домена.
4. Попробовать войти под своей учётной записью администратора на этом компьютере (для проверки локальной работоспособности).
5. Проверить в Active Directory, не заблокирована ли учётная запись, не истёк ли срок пароля.
6. Сбросить пароль или разблокировать учётную запись (если требуется).
7. Если всё равно не входит – проверить службы аутентификации (Kerberos, Netlogon).
8. Задokumentировать результат.

Ответ может быть сформулирован в другой близкой по смыслу формулировке

6.4 Ключи к вопросам для собеседования при проведении дифференцированного зачёта

1. Дайте определение сопровождения информационной системы. Перечислите основные задачи сопровождения.

Сопровождение информационной системы (ИС) – это комплекс мероприятий, направленных на поддержание работоспособности, производительности и актуальности системы в течение всего её жизненного цикла после ввода в эксплуатацию.

Основные задачи сопровождения:

- **Мониторинг** – непрерывное наблюдение за состоянием системы (доступность, загрузка, ошибки).
- **Резервное копирование и восстановление** – защита данных от потери.
- **Обновление ПО** – установка патчей, новых версий для устранения уязвимостей и расширения функционала.
- **Управление инцидентами** – быстрое реагирование на сбои и восстановление работы.
- **Управление проблемами** – поиск и устранение корневых причин инцидентов.
- **Обеспечение безопасности** – управление доступом, защита от атак.
- **Документирование** – ведение журналов, инструкций, базы знаний.
- **Консультирование пользователей** – помощь в работе с системой.

2. Какие виды резервного копирования вы знаете? Опишите их достоинства и недостатки.

Выделяют три основных типа:

Тип	Описание	Достоинства	Недостатки
Полное (Full)	Копируются все выбранные данные.	Восстановление самое быстрое (одна копия).	Требует много места и времени.
Инкрементное	Копируются только изменения с момента последнего бэкапа (любого типа).	Экономит место, быстрое выполнение.	Восстановление сложное – нужно применить все инкременты по цепочке.
Дифференциальное	Копируются изменения с момента последнего полного бэкапа.	Восстановление быстрее инкрементного (нужен только полный + последний дифференциальный).	Занимает больше места, чем инкрементное, с каждым разом растёт объём.

3. Что такое SLA, RTO и RPO? Как эти показатели связаны с планированием восстановления?

- **SLA (Service Level Agreement)** – соглашение об уровне обслуживания между поставщиком услуги и заказчиком. В нём фиксируются количественные метрики качества (время реакции, доступность, время восстановления и т.д.).
- **RTO (Recovery Time Objective)** – целевое время восстановления. Это максимально допустимое время простоя системы после сбоя. Определяет, как быстро нужно восстановить работоспособность.

- **RPO (Recovery Point Objective)** – целевая точка восстановления. Это максимально допустимый объём потери данных (т.е. на какой момент времени должны быть сохранены данные).
Определяет частоту резервного копирования.

Связь с планированием:

На основе требований SLA устанавливаются значения RTO и RPO. Чем жёстче RTO – тем дороже и сложнее инфраструктура (кластеры, горячие резервы). Чем меньше RPO – тем чаще нужно делать бэкапы. План аварийного восстановления разрабатывается так, чтобы гарантировать достижение этих показателей.

4. Опишите структуру плана аварийного восстановления (Disaster Recovery Plan).

План аварийного восстановления (DRP) – документ, регламентирующий действия по восстановлению ИТ-инфраструктуры после крупных катастроф (пожар, наводнение, кибератака, отказ оборудования).

Обязательные разделы:

1. **Цели и метрики** – RTO и RPO для каждой критичной системы.
2. **Список критических систем и приоритеты восстановления** – что восстанавливать в первую очередь.
3. **Схема оповещения и коммуникации** – кто и кого информирует, контакты.
4. **Роли и ответственность** – кто выполняет восстановление, кто принимает решения.
5. **Пошаговые процедуры восстановления** – для каждой системы (включая команды, последовательность действий).
6. **Ресурсы** – резервное оборудование, запасные носители, доступ к облачным хранилищам.
7. **План тестирования DRP** – как и когда проводятся учения по восстановлению.
8. **Порядок возврата к нормальной работе** – после восстановления.

5. Каковы основные обязанности системного администратора в процессе сопровождения ИС?

- Мониторинг работоспособности серверов и сетевого оборудования.
- Регулярное резервное копирование и проверка возможности восстановления.
- Установка обновлений и патчей безопасности.
- Управление учётными записями и правами доступа пользователей.
- Решение инцидентов (сбои, ошибки, запросы пользователей).
- Диагностика и устранение аппаратных и программных неисправностей.
- Ведение технической документации (журналы, инструкции, база знаний).
- Обеспечение информационной безопасности (настройка брандмауэров, антивирусов, анализ логов).
- Консультирование пользователей и обучение работе с системой.

6. Что такое инцидент и какова процедура его обработки? Чем инцидент отличается от проблемы?

Инцидент – это любое событие, которое не является частью стандартной работы услуги и вызывает или может вызвать перебой в её предоставлении.

Процедура обработки инцидента (стандарт ITIL):

1. **Регистрация** – фиксация факта, времени, описания.
2. **Классификация** – определение категории, приоритета, влияния.
3. **Диагностика** – сбор информации, поиск причины.
4. **Решение** – временное (workaround) или постоянное устранение.
5. **Закрытие** – подтверждение пользователем, документирование.

Отличие инцидента от проблемы:

- **Инцидент** – это единичное нарушение работы (например, «не открывается почта у одного пользователя»).
- **Проблема** – это корневая причина одного или нескольких инцидентов (например, «сбой службы

из-за утечки памяти»). Управление проблемами направлено на постоянное устранение причины, чтобы инциденты не повторялись.

7. Опишите процесс управления изменениями в ИС. Почему он важен?

Управление изменениями – это формализованный процесс внесения изменений в ИС (обновления, настройки, доработки) с оценкой рисков, согласованием и контролем.

Основные этапы:

1. **Инициация** – подача запроса на изменение (RFC).
2. **Оценка влияния** – анализ рисков, затрат, тестирование совместимости.
3. **Согласование** – утверждение Change Advisory Board (CAB).
4. **Планирование** – разработка плана внедрения и отката.
5. **Реализация** – выполнение изменений (по расписанию, часто в окно обслуживания).
6. **Тестирование** – проверка работоспособности после внедрения.
7. **Документирование** – обновление документации, закрытие запроса.

Почему важен:

- Снижает риск сбоев и простоев.
- Обеспечивает прозрачность и контроль.
- Позволяет откатить изменения при неудаче.
- Улучшает качество обслуживания и доверие заказчика.

8. Какие методы обеспечения безопасности информационной системы вы знаете?

- **Аутентификация и авторизация** – проверка пользователя и выдача прав.
- **Шифрование данных** – защита при передаче и хранении.
- **Межсетевые экраны (брандмауэры)** – фильтрация сетевого трафика.
- **Антивирусное и антишпионское ПО** – защита от вредоносных программ.
- **Регулярное обновление ПО** – закрытие уязвимостей.
- **Политика паролей** – сложность, срок действия, блокировка.
- **Многофакторная аутентификация (MFA)** – дополнительный фактор (SMS, токен, биометрия).
- **Системы обнаружения и предотвращения вторжений (IDS/IPS)** – мониторинг аномалий.
- **Аудит и журналирование** – запись действий для анализа и расследований.
- **Резервное копирование** – защита от потери данных.
- **Обучение пользователей** – повышение осведомлённости о фишинге и социальной инженерии.

9. Что такое аутентификация, авторизация и аудит? Приведите примеры.

Термин	Определение	Пример
Аутентификация	Проверка подлинности пользователя (подтверждение, что он тот, за кого себя выдаёт).	Ввод логина и пароля; сканирование отпечатка пальца.
Авторизация	Определение разрешённых действий и ресурсов, к которым пользователь имеет доступ.	После входа в систему пользователь может читать файлы в папке «Отчёты», но не может их изменять.
Аудит	Запись и анализ действий пользователей (кто, когда, что делал) для контроля и расследований.	Журнал безопасности Windows (Event Log) фиксирует неудачные попытки входа; системный администратор анализирует эти записи.

10. Какие существуют виды вредоносного ПО и как от них защищаться?

Основные виды:

- **Вирусы** – внедряются в исполняемые файлы, распространяются при запуске.
- **Черви** – самораспространяются по сети без участия пользователя.
- **Трояны** – маскируются под полезные программы, но выполняют скрытые вредоносные

действия.

- **Шифровальщики (Ransomware)** – шифруют файлы и требуют выкуп.
- **Шпионское ПО (Spyware)** – собирают конфиденциальную информацию.
- **Рекламное ПО (Adware)** – показывают назойливую рекламу.
- **Бэкдоры** – открывают скрытый доступ к системе злоумышленникам.

Методы защиты:

- Установка и регулярное обновление антивирусного ПО.
- Использование брандмауэра.
- Регулярная установка патчей безопасности.
- Ограничение прав пользователей (принцип наименьших привилегий).
- Обучение пользователей правилам безопасной работы (не открывать подозрительные письма и ссылки).
- Регулярное резервное копирование данных (для защиты от шифровальщиков).
- Использование систем обнаружения вторжений.

11. Что такое межсетевой экран (брандмауэр) и каковы его функции?

Межсетевой экран (брандмауэр, Firewall) – это устройство или программа, которая контролирует сетевой трафик на основе заданных правил безопасности, блокируя или разрешая соединения между сетями (например, между локальной сетью и Интернетом).

Основные функции:

- Фильтрация пакетов по IP-адресам, портам, протоколам.
- Контроль состояния соединений (stateful inspection) – разрешает только те пакеты, которые являются частью разрешённых сессий.
- Преобразование сетевых адресов (NAT) – скрывает внутреннюю структуру сети.
- Блокировка нежелательного трафика (защита от DDoS, сканирования портов).
- Ведение журнала событий для анализа атак.

12. Опишите процесс диагностики и устранения ошибок в ИС. Какие инструменты используются?

Общий алгоритм (Troubleshooting):

1. **Сбор информации** – опрос пользователя, сбор логов, мониторинг метрик.
2. **Воспроизведение проблемы** – попытка повторить ошибку в контролируемой среде.
3. **Анализ симптомов** – выделение ключевых признаков, поиск аномалий.
4. **Формулировка гипотез** – предположение о причинах.
5. **Тестирование гипотез** – проверка каждой (например, отключение служб, замена драйверов).
6. **Устранение причины** – внесение изменений (перезапуск, обновление, корректировка настроек).
7. **Проверка работоспособности** – тестирование системы после устранения.
8. **Документирование** – запись причин и решения.

Инструменты:

- **Системные утилиты:** Диспетчер задач, Event Viewer, Performance Monitor, Resource Monitor.
- **Сетевые:** ping, ipconfig, netstat, tracert, nslookup, Wireshark.
- **Дисковые:** chkdsk, sfc, дефрагментатор.
- **Мониторинговые:** Zabbix, Nagios, Prometheus.
- **Удалённое управление:** RDP, SSH, TeamViewer.

13. Что такое журналы событий (логи) и как они помогают в поиске ошибок?

Журналы событий (логи) – это системные файлы, в которые операционная система, приложения и службы записывают информацию о своей работе: ошибки, предупреждения, информационные сообщения, аудит безопасности.

Роль в поиске ошибок:

- Позволяют увидеть хронологию событий, предшествовавших сбою.
- Содержат коды ошибок, которые можно использовать для поиска решения.
- Помогают выявить закономерности (например, ошибка возникает в определённое время).
- Дают информацию о состоянии системы на момент сбоя (загрузка, память).
- Используются для расследования инцидентов безопасности.

Пример: в Windows Event Viewer (журнал «Система») можно найти запись с кодом ошибки, которая укажет на проблемный драйвер или службу.

14. Какие встроенные утилиты Windows вы знаете для мониторинга и диагностики?

- **Диспетчер задач (Task Manager)** – просмотр запущенных процессов, загрузка CPU, памяти, диска, сети.
- **Просмотр событий (Event Viewer)** – просмотр системных, прикладных и защитных логов.
- **Монитор производительности (Performance Monitor)** – графики и счётчики для детального анализа нагрузки.
- **Монитор ресурсов (Resource Monitor)** – детальная информация об использовании CPU, памяти, диска, сети.
- **Командная строка (cmd) и PowerShell** – для работы с утилитами:
 - ping – проверка доступности узлов.
 - ipconfig – просмотр и обновление IP-конфигурации.
 - netstat – просмотр открытых портов и сетевых соединений.
 - tracert – трассировка маршрута.
 - chkdsk – проверка целостности диска.
 - sfc /scannow – проверка системных файлов.
 - wmic – получение информации об оборудовании.

15. Как определить, что причина сбоя – аппаратная, а не программная?

Признаки аппаратного сбоя:

- Система не включается или включается, но не загружается (чёрный экран, отсутствие сигнала на монитор).
- Постоянные ошибки чтения/записи, появление битых секторов на диске (проверить через chkdsk или S.M.A.R.T.).
- Компьютер перегревается, шум от кулеров, запах гари.
- «Синий экран смерти» с критическими кодами ошибок, указывающими на память (например, MEMORY_MANAGEMENT) или диск (INACCESSIBLE_BOOT_DEVICE).
- Перезагрузки под нагрузкой (проблемы с блоком питания).
- Не определяется оборудование в BIOS/UEFI.

Методы проверки:

- Загрузиться с Live-CD или загрузочной флешки – если проблема исчезает, то причина в программах или драйверах.
- Запустить диагностику памяти (Windows Memory Diagnostic, MemTest86).
- Проверить диск через утилиты производителя (CrystalDiskInfo, HDDScan).
- Заменить подозрительный компонент на заведомо исправный (метод замены).

16. Что такое «синий экран смерти» и как анализировать его причины?

«Синий экран смерти» (BSOD – Blue Screen of Death) – это критическая ошибка ядра Windows, приводящая к аварийной остановке системы для предотвращения повреждения данных.

Анализ причин:

1. Записать код ошибки (STOP-код) и параметры, которые отображаются на экране (или найти в дампе памяти).
2. Восстановить недавние изменения: обновления, драйверы, новое оборудование (откатить или удалить).

3. Проверить системный журнал событий (Event Viewer) – найти записи, предшествующие BSOD.
4. Проанализировать файл дампа памяти (можно использовать WinDbg или BlueScreenView) – он показывает, какой модуль вызвал ошибку.
5. Проверить оборудование: память (MemTest), диск (chkdsk), перегрев, блок питания.
6. Обновить драйверы устройств (особенно видеокарта, сетевые адаптеры).
7. Если ничего не помогает – выполнить восстановление системы до предыдущей контрольной точки.

17. Опишите алгоритм действий при потере сетевого подключения у пользователя.

1. **Уточнить у пользователя симптомы:** что не открывается, есть ли доступ к локальным ресурсам, другие компьютеры работают?
2. **Проверить физическое подключение:** кабель подключён, индикатор на сетевой карте горит, Wi-Fi включён.
3. **Выполнить команду ipconfig** – посмотреть, есть ли IP-адрес (если начинается с 169.254 – проблема с DHCP).
4. **Выполнить ping 127.0.0.1** – проверка работоспособности сетевой карты (loopback).
5. **Выполнить ping <IP-адрес шлюза>** – проверка связи с маршрутизатором.
6. **Выполнить ping 8.8.8.8** – проверка доступа в Интернет.
7. **Выполнить nslookup yandex.ru** – проверка работы DNS.
8. Если шлюз не пингуется – проверить настройки DHCP, перезагрузить маршрутизатор, заменить кабель.
9. Если DNS не работает – проверить настройки DNS-сервера, возможно, задать статический DNS (например, 8.8.8.8).
10. Если всё перечисленное не помогает – использовать tracert для определения места обрыва.
11. При необходимости – переустановить драйвер сетевой карты или проверить наличие конфликтов IP-адресов.
12. Задokumentировать проблему и решение.

18. Почему важно документировать все действия по устранению ошибок?

Документирование действий по устранению ошибок – это критически важный процесс, который обеспечивает:

- **Накопление опыта** – создаётся база знаний, где хранятся решения типовых проблем, что ускоряет их обработку в будущем.
- **Обучение новых сотрудников** – новички могут использовать документацию как обучающий материал, сокращая время вводного курса.
- **Снижение повторяемости** – если причина и решение задокументированы, другие администраторы не тратят время на повторную диагностику.
- **Анализ и улучшение** – по статистике документированных инцидентов можно выявить слабые места системы и провести профилактику.
- **Соблюдение нормативных требований** – во многих отраслях (финансы, медицина) требуется вести журналы действий для аудита.
- **Юридическая защита** – в случае спорных ситуаций документация подтверждает, что работы выполнялись квалифицированно и в установленные сроки.

Все ответы могут быть сформулированы в другой близкой по смыслу формулировке

6.5 Ключи на вопросы для устного опроса

1. Дайте определение сопровождения информационной системы. Каковы его основные цели?

Сопровождение информационной системы (ИС) – это комплекс мероприятий, выполняемых после ввода системы в эксплуатацию, направленных на поддержание её работоспособности,

производительности, безопасности и соответствия изменяющимся требованиям пользователей и бизнеса.

Основные цели сопровождения:

- **Обеспечение бесперебойной работы** – минимизация простоев и сбоев.
- **Сохранность данных** – защита от потери, повреждения или утечки.
- **Адаптация к изменениям** – обновление функционала, интеграция с новыми системами.
- **Повышение эффективности** – оптимизация производительности, улучшение пользовательского опыта.
- **Соответствие нормативам** – соблюдение законодательных и отраслевых требований (безопасность, хранение данных).

2. Что такое инцидент в IT? Чем он отличается от проблемы?

Инцидент – это любое событие, которое не является частью стандартной работы услуги и вызывает или может вызвать перебой в её предоставлении (например, недоступность сайта, ошибка при открытии файла, сбой в работе приложения).

Отличие от проблемы:

- **Инцидент** – это единичное проявление сбоя. Его цель – быстро восстановить услугу (временное решение).
- **Проблема** – это корневая причина одного или нескольких инцидентов. Её цель – найти и устранить первопричину, чтобы инциденты не повторялись.

Пример: Инцидент – «пользователь не может войти в систему». Проблема – «учётная запись блокируется из-за неправильной политики истечения пароля, которая не обновляется».

3. Опишите основные этапы обработки инцидента.

Стандартный процесс (по ITIL) включает следующие этапы:

1. **Регистрация** – фиксация факта инцидента (время, описание, данные пользователя).
2. **Классификация** – определение категории, приоритета, влияния на бизнес.
3. **Диагностика** – сбор дополнительной информации, анализ симптомов, попытка воспроизведения.
4. **Решение** – применение временного обходного решения (workaround) или постоянного исправления.
5. **Закрытие** – подтверждение пользователем, что проблема решена, документирование всех действий.
6. **Эскалация** (при необходимости) – передача инцидента на более высокий уровень поддержки, если не удаётся решить на текущем уровне.

4. Что такое Соглашение об уровне обслуживания (SLA) и какую роль оно играет?

Соглашение об уровне обслуживания (SLA, Service Level Agreement) – это официальный документ между поставщиком IT-услуг и заказчиком, который определяет количественные и качественные показатели предоставляемых услуг.

Роль SLA:

- Устанавливает чёткие ожидания и обязательства сторон.
- Содержит метрики: доступность системы (%), например, 99.9%, время реакции на инцидент, время восстановления (RTO), частота резервного копирования и т.д.
- Служит основой для контроля качества и выставления счетов (в случае коммерческих услуг).
- Помогает избежать споров, так как все критерии заранее формализованы.

5. Что такое резервное копирование и каковы его основные цели?

Резервное копирование (Backup) – это процесс создания копии данных, которая может быть использована для восстановления в случае их потери, повреждения или несанкционированного доступа.

Основные цели:

- **Защита от сбоев оборудования** (отказ жёсткого диска, повреждение RAID).
- **Восстановление после атак** (шифровальщики, вирусы).
- **Сохранение данных при человеческих ошибках** (случайное удаление или изменение).
- **Обеспечение непрерывности бизнеса** – возможность быстро возобновить работу после катастрофы.
- **Соблюдение нормативных требований** (например, обязательное хранение архивов в течение определённого срока).

6. В чём разница между полным, инкрементным и дифференциальным резервным копированием?

Тип	Описание	Особенности
Полное (Full)	Копируются все выбранные данные каждый раз.	Занимает много места и времени. Восстановление самое быстрое (достаточно одной копии).
Инкрементное (Incremental)	Копируются только изменения с момента последнего резервного копирования (любого типа).	Экономит место, быстро выполняется. Восстановление требует последовательного применения всех инкрементов от последнего полного.
Дифференциальное (Differential)	Копируются только изменения с момента последнего полного резервного копирования.	Занимает больше места, чем инкрементное (объём растёт до следующего полного). Восстановление быстрее – нужны только последний полный и последний дифференциальный бэкап.

7. Объясните разницу между целевым временем восстановления (RTO) и целевой точкой восстановления (RPO).

- **RTO (Recovery Time Objective)** – целевое время восстановления. Это максимально допустимый период простоя системы (время, за которое нужно восстановить работоспособность после сбоя). Влияет на выбор средств быстрого восстановления (кластеры, репликация, горячие резервы).
- **RPO (Recovery Point Objective)** – целевая точка восстановления. Это максимально допустимый объём потери данных (т.е. на какой момент времени мы можем восстановить данные). Определяет частоту резервного копирования – чем меньше RPO, тем чаще нужно делать бэкапы.

Связь: Оба показателя используются в плане аварийного восстановления. RTO влияет на стоимость инфраструктуры (чем меньше время, тем дороже), RPO – на интенсивность резервирования.

8. Что такое план аварийного восстановления и какие ключевые элементы он должен включать?

План аварийного восстановления (Disaster Recovery Plan, DRP) – это документированный набор процедур и инструкций, обеспечивающих восстановление критичных ИТ-систем и данных после крупных сбоев или катастроф (пожар, наводнение, кибератака, отказ оборудования).

Ключевые элементы:

1. **Цели восстановления** – RTO и RPO для каждой системы.
2. **Приоритеты** – какие системы восстанавливать в первую очередь (критические).
3. **Роли и ответственность** – состав команды, контакты, кто принимает решения.
4. **Процедуры восстановления** – пошаговые инструкции (включая команды, последовательность действий).
5. **Ресурсы** – резервное оборудование, доступ к внешним хранилищам, лицензии.

6. **Схема коммуникации** – кто и как оповещается о катастрофе (внутренние и внешние стейкхолдеры).
7. **План тестирования** – как часто проводятся учения по отработке восстановления.
8. **Возврат к нормальной работе** – процедуры переключения обратно на основную инфраструктуру.

9. Для чего используются контрольные точки восстановления в операционных системах?

Контрольные точки восстановления (System Restore Points) – это «снимки» состояния системных файлов, настроек реестра и установленных приложений на определённый момент времени. Они создаются автоматически (перед установкой обновлений, драйверов) или вручную.

Назначение:

- **Откат системы** – позволяют вернуть ОС к рабочему состоянию в случае неудачной установки обновления, драйвера или программного обеспечения.
- **Безопасное тестирование** – перед внесением значительных изменений можно создать точку, чтобы иметь возможность отменить изменения.
- **Ускорение восстановления** – вместо полной переустановки системы можно быстро откатиться к предыдущему стабильному состоянию.

Важно: Точки восстановления не заменяют полноценное резервное копирование пользовательских данных (они не сохраняют личные файлы).

10. Что такое отказоустойчивый кластер и как он повышает доступность системы?

Отказоустойчивый кластер – это группа независимых серверов (узлов), которые работают совместно, предоставляя общий сервис, и в случае отказа одного узла нагрузка автоматически переключается на другие узлы без заметного простоя для пользователей.

Как повышает доступность:

- **Аппаратная избыточность** – отказ одного сервера не приводит к остановке всей системы.
- **Автоматическое переключение (failover)** – при обнаружении сбоя происходит переключение на резервный узел.
- **Балансировка нагрузки** – распределение запросов между узлами повышает общую производительность.
- **Плановое обслуживание** – можно проводить обновления на одном узле, не выключая сервис для пользователей.

Пример: кластер баз данных с двумя узлами и общим дисковым хранилищем.

11. Перечислите основные обязанности системного администратора.

- Мониторинг работоспособности серверов, сетевого оборудования и ПО.
- Регулярное резервное копирование данных и проверка восстановления.
- Установка и настройка программного обеспечения, обновлений, патчей.
- Управление учётными записями пользователей и правами доступа.
- Оперативное решение инцидентов (сбои, ошибки, запросы).
- Диагностика и устранение аппаратных и программных неисправностей.
- Обеспечение информационной безопасности (настройка брандмауэров, антивирусов, анализ логов).
- Документирование конфигураций, процедур, инцидентов.
- Консультирование и обучение пользователей.
- Участие в планировании развития ИТ-инфраструктуры (закупки, модернизация).

12. Что подразумевается под информационной безопасностью? Назовите три её ключевых аспекта (CIA-триада).

Информационная безопасность – это совокупность методов и средств, обеспечивающих защиту информации от несанкционированного доступа, модификации, уничтожения или раскрытия.

Три ключевых аспекта (CIA-триада):

- **Конфиденциальность (Confidentiality)** – гарантия того, что информация доступна только авторизованным лицам. Обеспечивается шифрованием, контролем доступа, аутентификацией.
- **Целостность (Integrity)** – защита от несанкционированного изменения или уничтожения данных. Обеспечивается хешированием, контрольными суммами, ограничением прав на запись.
- **Доступность (Availability)** – гарантия того, что система и данные доступны авторизованным пользователям в нужное время. Обеспечивается резервированием, быстрым восстановлением, защитой от DDoS-атак.

13. Объясните разницу между аутентификацией и авторизацией.

- **Аутентификация (Authentication)** – это процесс проверки подлинности пользователя, подтверждение его личности. Отвечает на вопрос «Кто ты?». Обычно выполняется через логин/пароль, сертификаты, биометрию.
- **Авторизация (Authorization)** – это процесс определения прав и разрешений для аутентифицированного пользователя. Отвечает на вопрос «Что тебе разрешено?». Проверяется, к каким ресурсам (файлы, базы данных, функции) пользователь имеет доступ.

Пример: При входе в систему вы вводите логин и пароль – это **аутентификация**. После входа вы можете просматривать свою электронную почту, но не можете изменять настройки сервера – это **авторизация**.

14. Что такое политика паролей и какие современные требования к ним предъявляются?

Политика паролей – это набор правил, регулирующих создание, использование и хранение паролей в организации, обеспечивающий их надёжность и защиту от взлома.

Современные требования (рекомендации NIST, Microsoft):

- Минимальная длина – не менее 8 символов (рекомендуется 12–16).
- Запрет на простые и распространённые пароли (например, "qwerty", "password", "123456").
- Требование использовать комбинацию букв (верхний/нижний регистр), цифр и специальных символов – *но* это не всегда обязательно при достаточной длине.
- Ограничение на количество неудачных попыток входа (блокировка на 5–10 попыток).
- Истечение срока действия пароля (например, каждые 90 дней) – сейчас критикуется, рекомендуется менять только при компрометации.
- Запрет на использование одного пароля для нескольких систем.
- Хранение паролей в хешированном виде с солью.

15. Что такое многофакторная аутентификация и почему она эффективнее однофакторной?

Многофакторная аутентификация (MFA) – это метод проверки подлинности, требующий предоставления двух или более независимых факторов подтверждения личности.

Три основных фактора:

- **Знание** (что-то, что вы знаете) – пароль, PIN-код.
- **Владение** (что-то, что у вас есть) – смарт-карта, одноразовый код из приложения (Google Authenticator), SMS.
- **Врождённое** (что-то, что вы есть) – биометрия (отпечаток пальца, сканер лица, радужка).

Почему эффективнее однофакторной:

- Злоумышленнику нужно скомпрометировать как минимум два независимых фактора (например, украсть пароль и физический токен или подделать биометрию), что значительно сложнее.
- Даже если пароль стал известен (например, через фишинг), без второго фактора доступ будет невозможен.
- Снижает риск несанкционированного доступа при краже базы данных паролей.

16. Каковы основные задачи межсетевого экрана (брандмауэра)?

Межсетевой экран (брандмауэр, Firewall) – это устройство или программа, которая фильтрует

сетевой трафик между различными сетями (например, между локальной сетью и Интернетом) на основе заданных правил.

Основные задачи:

- **Фильтрация пакетов** – разрешение или блокировка соединений по IP-адресам, портам, протоколам (TCP, UDP, ICMP).
- **Контроль состояния соединений (Stateful Inspection)** – отслеживание активных сессий и разрешение только тех пакетов, которые относятся к уже установленным соединениям.
- **Преобразование сетевых адресов (NAT)** – скрытие внутренней структуры сети, сопоставление публичного IP-адреса с внутренними адресами.
- **Защита от несанкционированного доступа** – блокировка попыток сканирования портов, атак типа "отказ в обслуживании" (DDoS).
- **Ведение журнала** – запись событий (разрешённых и запрещённых соединений) для последующего анализа и аудита.

17. Что такое система обнаружения и предотвращения вторжений?

Система обнаружения вторжений (IDS, Intrusion Detection System) – это программное или аппаратное средство, которое анализирует сетевой трафик или активность системы и выявляет подозрительные действия, признаки атак или нарушения политики безопасности. IDS **только обнаруживает** и сигнализирует, но не блокирует.

Система предотвращения вторжений (IPS, Intrusion Prevention System) – это более продвинутое средство, которое не только обнаруживает, но и **автоматически блокирует** подозрительный трафик или активность в реальном времени.

Общие функции:

- Мониторинг сетевого трафика и системных логов.
- Сравнение с сигнатурами известных атак (сигнатурный анализ).
- Выявление аномалий (поведенческий анализ) – отклонения от нормального поведения.
- В случае IPS – автоматическое прерывание соединения, блокировка IP, отправка предупреждений администратору.

18. Для чего необходима установка патчей и обновлений безопасности?

Патчи и обновления безопасности – это исправления, выпускаемые разработчиками ПО для устранения обнаруженных уязвимостей, ошибок и улучшения стабильности.

Необходимость:

- **Заккрытие уязвимостей** – предотвращение эксплуатации известных дыр злоумышленниками (например, уязвимости, по которым выпускаются эксплойты).
- **Повышение стабильности** – исправление ошибок, вызывающих сбои и зависания.
- **Улучшение производительности** – иногда обновления содержат оптимизации.
- **Соответствие стандартам** – многие регуляторы (например, PCI DSS) требуют своевременного обновления ПО.
- **Защита от новых угроз** – регулярные патчи снижают риск успешных атак, особенно на широко используемые системы (ОС, браузеры, веб-серверы).

Рекомендация: устанавливать патчи в тестовой среде перед внедрением в продуктивную, иметь план отката на случай проблем.

Все ответы могут быть сформулированы в другой близкой по смыслу формулировке