



Министерство образования Республики Марий Эл  
Государственное бюджетное профессиональное  
Общеобразовательное учреждение  
Республики Марий Эл  
«Марийский радиомеханический техникум»

## ОТЧЕТ ПО ПРОИЗВОДСТВЕННОЙ ПРАКТИКЕ

ПП.04.01.09.02.07-009

### **ПМ.04 Сопровождение и обслуживание программного обеспечения компьютерных систем**

Выполнил  
студент группы П-31  
\_\_\_\_\_ Кадыков Р.В.

Руководитель практики  
\_\_\_\_\_ Матвеева Е.В.

Руководитель практики  
от предприятия  
\_\_\_\_\_ Гурев А.Е.

ГБПОУ Республики Марий Эл  
«Марийский радиомеханический техникум»

## ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ

На период производственной практики с «19» мая 2025 г. по «9» июня 2025 г. студента группы П-31 специальности 09.02.07 Информационные системы и программирование Кадыкова Романа Владимировича по ПМ.04 Сопровождение и обслуживание программного обеспечения компьютерных систем

Вопросы, подлежащие изучению:

- ГОСТ Р ИСО/МЭК 12207. Основные процессы и взаимосвязь между документами в информационной системе согласно стандартам;
- Осуществлять инсталляцию, настройку и обслуживание программного обеспечения компьютерных систем;
- Выполнять измерение эксплуатационных характеристик программного обеспечения компьютерных систем;
- Выполнять работы по модификации отдельных компонент программного обеспечения в соответствии с потребностями заказчика;
- Участвовать в обеспечении защиты программного обеспечения компьютерных систем программными средствами;
- Участвовать в инспектировании компонент программного обеспечения на предмет соответствия стандартам кодирования.

Руководители практики:

от предприятия

Гурев Александр Евгеньевич

(фамилия, имя, отчество)

от техникума

Матвеева Елена Владимировна

(фамилия, имя, отчество)

# СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....	4
1 Ознакомительный этап .....	5
1.1 Структура организации .....	5
1.2 Охрана труда и техника безопасности .....	5
1.3 Описание рабочего места .....	8
1.4 ГОСТ Р ИСО/МЭК 12207. Основные процессы и взаимосвязь между документами в информационной системе согласно стандартам .....	9
2 Производственный этап.....	15
2.1 Участвовать в документировании процессов инсталляции, настройки, обслуживания ПО и результатов мониторинга эксплуатационных характеристик .....	15
2.2 Диагностировать проблемы производительности и безопасности программного обеспечения компьютерных систем и участвовать в их оптимизации .....	18
2.3 Оказывать техническую поддержку пользователям и устранять неисправности в работе программного обеспечения компьютерных систем .....	21
ЗАКЛЮЧЕНИЕ .....	23
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ .....	26

					ПП.04.01.09.02.07-009		
Изм.	Лист	№ докум.	Подпись	Дата	Лит.	Лист	Листов
Разраб.	<i>Кадыков Р.В</i>					3	28
Проверил	<i>Матвеева Е.В.</i>						
Реценз.							
Н. Контр.	<i>Матвеева Е.В.</i>						
Утв.							
ОТЧЕТ ПО ПРОИЗВОДСТВЕННОЙ ПРАКТИКЕ					МРМТ П-31		

## ВВЕДЕНИЕ

Сопровождение и техническая поддержка программного обеспечения играют критически важную роль в обеспечении бесперебойной работы современных информационных систем. Эти процессы охватывают не только первоначальную инсталляцию и конфигурирование программных решений, но и их регулярное обновление, техническую поддержку и совершенствование в соответствии с потребностями пользователей и динамично развивающейся технологической средой.

В эпоху стремительного технологического прогресса вопросы обеспечения стабильности и защищенности программных продуктов приобретают особую значимость. Основными приоритетами в этой сфере становятся мониторинг качества работы систем, поддержание заявленных эксплуатационных параметров и кастомизация программных решений под индивидуальные требования заказчиков. Следовательно, организация эффективного сопровождения ПО требует системного подхода и профессиональной экспертизы в сфере информационных технологий.

Подобная практическая деятельность дает бесценный опыт для детального изучения этих процессов и реализации теоретических знаний в реальных условиях, что составляет важнейшую часть профессионального становления специалистов в области программирования и информационных систем.

Изм.	Лист	№ докум.	Подпись	Дата	ПП.04.01.09.02.07-009	Лист 4
------	------	----------	---------	------	-----------------------	-----------

# 1 Ознакомительный этап

## 1.1 Структура организации

ПАО «Ростелеком» - телекоммуникационная компания, провайдер цифровых услуг. Структура организации представлена на рисунке 1.

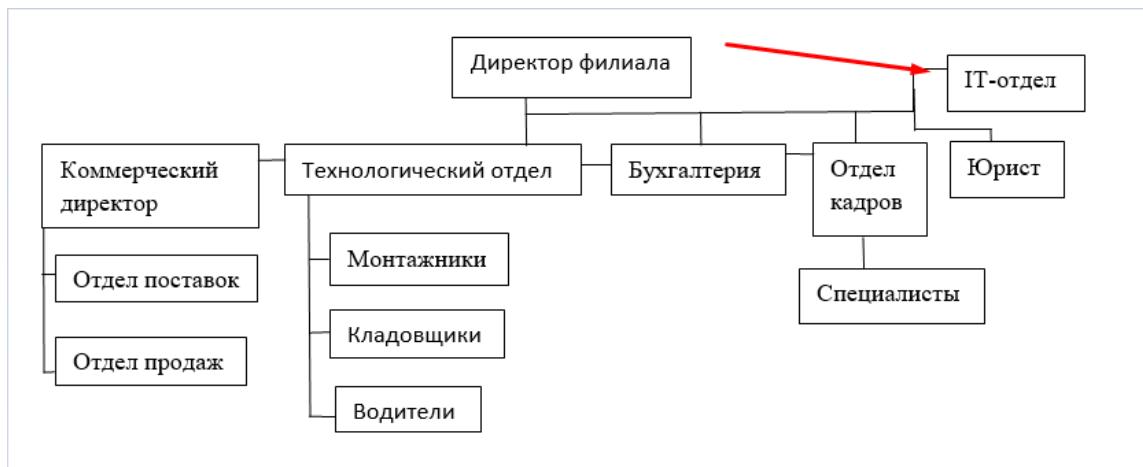


Рисунок 1 – Структура организации «ПАО Ростелеком»

## 1.2 Охрана труда и техника безопасности

Во время прохождения практики на предприятии связи ПАО «Ростелеком» были организованы работы и контроль за выполнением мероприятий по охране труда. Контроль за соблюдением правил техники безопасности и выполнением соответствующих мероприятий осуществляют главный инженер и инженер по технике безопасности.

На предприятиях связи должны производиться следующие мероприятия по охране труда:

- 1) Составление ежегодных планов мероприятий по охране труда.
- 2) Составление санитарно-технических паспортов на производственные помещения.

Изм.	Лист	№ докум.	Подпись	Дата	ПП.04.01.09.02.07-009	Лист
						5

3) Аттестация рабочих мест, переоборудованного или вновь установленного оборудования.

4) Расследование и учет несчастных случаев.

5) Проведение периодических (один раз в два года) медосмотров работников, связанных с обслуживанием электрооборудования.

6) Обучение и проверка по технике безопасности (ежегодно).

7) Утверждение списка лиц, не связанных с обслуживанием оборудования, т.е. не подлежащих проверке по технике безопасности, утверждение профессий и должностей, с которыми не проводится первичный инструктаж на рабочем месте.

8) Организация проверок электрозащитных средств, защитного заземления, сопротивления изоляции питающих проводов, первичных средств пожаротушения и т.д.

9) Проведение смотровых конкурсов по охране труда.

10) Проведение трехступенчатого контроля.

Первая ступень проводится ежедневно мастером или бригадиром. Проверяется состояние рабочих мест, исправность оборудования и защитных средств. При обнаружении недостатков немедленно принимаются меры по их устранению. Если устранить неисправность своими силами не представляется возможным, то выявленные нарушения записываются в журнал трехступенчатого контроля.

Вторая ступень проводится еженедельно. Начальник цеха проводит детальную проверку состояния охраны труда в цехе, принимает решения по замечаниям, сделанным мастером, и контролирует выполнение мероприятий по устранению недостатков, выявленных при предыдущих проверках. Результаты проверки начальник цеха записывает в журнал второй ступени.

Третья ступень — ежеквартальная. Главный инженер и инженер по технике безопасности проверяют состояние охраны труда в целом по предприятию, контролируют устранение недостатков, выявленных на первой и

Изм.	Лист	№ докум.	Подпись	Дата
------	------	----------	---------	------

второй ступенях проверки. Результаты оформляются, составляется акт, и если имеется грубое нарушение, издается приказ по предприятию.

Дополнительные мероприятия по охране труда включают:

- 1) Составление отчета по производственному травматизму.
- 2) Составление актов классификации помещений по степени электробезопасности (проводится приказом по предприятию).
- 3) Финансирование и планирование мероприятий по охране труда и внедрение стандартов безопасности труда.

Для уменьшения случаев производственного травматизма на предприятиях связи проводятся инструктажи. Существуют следующие виды инструктажей:

- 1) Вводный инструктаж — проводится при поступлении на работу инженером по технике безопасности по программе, утвержденной руководителем предприятия. Оформляется в контрольном листе, который хранится в личном деле работника.
- 2) Первичный инструктаж на рабочем месте — проводится также при поступлении на работу и оформляется в контрольном листе. Для работников, связанных с электрооборудованием, в течение 10-12 смен проводится стажировка на рабочем месте.
- 3) Повторный инструктаж — проводится раз в полгода, а в строительных организациях — раз в три месяца.
- 4) Внеплановый инструктаж — проводится в случае, если изменилось оборудование, произошел несчастный случай или работник отсутствовал на своем рабочем месте более трех месяцев.
- 5) Целевой инструктаж — проводится при выполнении разовых работ с повышенной опасностью или особо опасных.

Изм.	Лист	№ докум.	Подпись	Дата
------	------	----------	---------	------

ПП.04.01.09.02.07-009

Лист

### **1.3 Описание рабочего места**

Рабочее место организовано на стандартном офисном столе, обеспечивающем достаточную площадь для размещения компьютерной техники и документов.

Рабочее место оснащено эргономичным офисным креслом с регулировкой высоты, что обеспечивает соблюдение требований к организации рабочего пространства и создает комфортные условия для продолжительной работы за компьютером.

ПК имеет следующие характеристики:

- Процессор Intel Core i5-10400, 6 ядер, базовая частота 2.9 ГГц и 4.3 ГГц в Turbo Boost. Обеспечивает достаточную мощность для обработки офисных приложений и одновременной работы с несколькими задачами.
- Оперативная память на 8 ГБ, DDR4, позволяет комфортно работать с офисными приложениями, веб-браузерами и средними объемами данных.
- SSD на 500 ГБ обеспечивает быструю загрузку ОС и приложений, а HDD предоставляет больше пространства для хранения документов и файлов.
- Интегрированная видеокарта Intel UHD Graphics 630 подходит для офисной работы, просмотра видео и использования стандартных графических приложений.
- Операционная система Windows 10 Pro обеспечивает безопасность и доступ ко всем необходимым инструментам для работы.
- Стандартная USB-клавиатура с мембранными переключателями обеспечивает комфортный набор текста и надежность в работе.
- Оптическая USB-мышь удобно лежит в руке и поддерживает стандартные функции, необходимые для работы.

Изм.	Лист	№ докум.	Подпись	Дата	ПП.04.01.09.02.07-009	Лист
						8

## **1.4 ГОСТ Р ИСО/МЭК 12207. Основные процессы и взаимосвязь между документами в информационной системе согласно стандартам**

Стандарт ГОСТ Р ИСО/МЭК 12207 (адаптированная версия ISO/IEC 12207) представляет собой нормативный документ, регулирующий все процессы жизненного цикла программного обеспечения. Он предназначен для систематизации и управления этапами от возникновения потребности в программном обеспечении до прекращения его эксплуатации. Стандарт широко применяется в российских и международных ИТ-проектах, обеспечивая единый подход к созданию и сопровождению информационных систем.

Применение ГОСТ Р ИСО/МЭК 12207 позволяет устанавливать четкие правила взаимодействия между участниками разработки, а также упрощает интеграцию проектной деятельности в бизнес-процессы организации. Его положения охватывают как технические, так и организационные аспекты, что делает его универсальным инструментом для управления проектами в области информационных технологий.

Стандарт способствует достижению следующих целей:

- упорядочивает процессы проектирования, разработки и сопровождения программных решений;
- обеспечивает соответствие создаваемого программного обеспечения установленным требованиям;
- способствует достижению управляемости проектов и минимизации рисков при реализации сложных программных систем;
- поддерживает интеграцию с другими стандартами, такими как ISO/IEC 15288.

ГОСТ Р ИСО/МЭК 12207 прошел несколько этапов развития. Первая версия международного стандарта была принята в 1995 году. В 2008 году

Изм.	Лист	№ докум.	Подпись	Дата	ПП.04.01.09.02.07-009	Лист 9
------	------	----------	---------	------	-----------------------	-----------

документ был переработан с целью интеграции с системной инженерией. В России действует редакция 2010 года, принятая в статусе национального стандарта.

Стандарт делит все процессы, входящие в жизненный цикл программного обеспечения, на три основные категории: основные, вспомогательные и организационные. Каждая из них играет важную роль в обеспечении успешной реализации проекта.

Основные категории процессов:

- 1) основные процессы охватывают ключевые этапы жизненного цикла, включая заказ, поставку, разработку, эксплуатацию и сопровождение программного обеспечения.
- 2) вспомогательные процессы обеспечивают поддержку выполнения основных процессов и включают управление конфигурацией, верификацию, валидацию и документирование.
- 3) организационные процессы направлены на общее управление проектом, включая планирование, управление ресурсами и обучение персонала.

Эта структура процессов способствует эффективному распределению ответственности между участниками проекта и повышает прозрачность действий на всех этапах разработки и сопровождения программного обеспечения.

Основные процессы стандарта определяют этапы, напрямую связанные с жизненным циклом программного обеспечения. Каждый из них имеет четко очерченную цель и результат.

Основными процессами являются:

- 1) Процесс заказа включает формулировку требований, выбор поставщика и заключение договора.
- 2) Процесс поставки охватывает разработку плана, реализацию программного обеспечения и его передачу заказчику.

Изм.	Лист	№ докум.	Подпись	Дата
------	------	----------	---------	------

3) Процесс разработки охватывает анализ требований, проектирование, реализацию, тестирование и интеграцию компонентов.

4) Процесс эксплуатации направлен на настройку системы, обучение пользователей и обеспечение стабильной работы программного обеспечения.

5) Процесс сопровождения включает обновление, устранение ошибок, адаптацию к изменяющимся условиям и завершение жизненного цикла системы.

Например, в проекте по автоматизации бухгалтерского учета заказ формулирует ключевые бизнес-требования, разработка включает реализацию соответствующих функций, а сопровождение обеспечивает корректную работу при изменении законодательства.

Вспомогательные процессы выполняются параллельно с основными и служат для обеспечения качества, стабильности и управляемости проекта.

Основные вспомогательные процессы включают:

- управление конфигурацией, которое обеспечивает контроль версий и отслеживание изменений программного обеспечения;
- верификацию, позволяющую подтвердить, что программный продукт соответствует установленным спецификациям;
- валидацию, направленную на проверку соответствия ожиданиям пользователей и условиям эксплуатации;
- документирование, включающее разработку руководств, инструкций и других материалов, необходимых для эффективного использования системы.

Эти процессы позволяют своевременно выявлять и устранять несоответствия, минимизируя риски и затраты на этапе внедрения.

Организационные процессы ориентированы на управление проектной деятельностью в целом. Они обеспечивают создание условий для выполнения основных и вспомогательных процессов.

Состав организационных процессов включает:

Изм.	Лист	№ докум.	Подпись	Дата
------	------	----------	---------	------

- 1) планирование сроков, этапов и ресурсов, необходимых для выполнения проекта;
- 2) обеспечение инфраструктуры, включая выбор инструментов разработки, лицензий и оборудования;
- 3) обучение персонала, направленное на повышение квалификации и адаптацию сотрудников к требованиям проекта;
- 4) управление рисками, которое помогает прогнозировать и предотвращать возможные проблемы на ранних стадиях.

Комплексное выполнение этих процессов способствует достижению проектных целей и оптимизации затрат.

На каждом этапе жизненного цикла программного обеспечения формируются документы, фиксирующие принятые решения, технические характеристики и порядок взаимодействия участников проекта.

Документирование этапа заказа включает:

- техническое задание, в котором формализуются цели, требования и ограничения проекта;
- договор, определяющий сроки, стоимость, условия приемки и ответственность сторон.

Документирование этапа разработки включает:

- спецификацию требований (SRS), содержащую описание функций и сценариев работы системы;
- архитектурное описание, включающее схемы компонентов, интерфейсы и используемые технологии;
- документацию кода, API, а также тест-планы и тест-кейсы, описывающие порядок проверки системы.

Документирование этапа эксплуатации включает:

- руководство пользователя, содержащее инструкции по работе с интерфейсом;

Изм.	Лист	№ докум.	Подпись	Дата

- административное руководство, описывающее настройки и обслуживание системы;
- регламент эксплуатации, определяющий правила обновлений и реагирования на инциденты.

Документирование этапа сопровождения включает:

- журнал изменений, в котором отражаются модификации версий программного обеспечения;
- отчеты об ошибках, фиксирующие проблемы и ход их устранения;
- план вывода из эксплуатации, описывающий действия при окончании жизненного цикла системы.

Все документы логически связаны между собой. Например, требования из технического задания формируют основу спецификаций, архитектурных решений и тест-кейсов. Обновления программного обеспечения требуют синхронного обновления пользовательских инструкций и эксплуатационной документации. Отсутствие актуальности в одном из документов может повлечь за собой ошибки на других этапах.

ГОСТ Р ИСО/МЭК 12207 широко применяется в организациях различного масштаба. Его гибкость позволяет адаптировать структуру под конкретные условия. В крупных ИТ-проектах соблюдаются все процессы стандарта, тогда как в стартапах или при разработке минимально жизнеспособного продукта (MVP) допускается объединение и упрощение этапов.

Примеры практического применения:

- 1) В крупных корпоративных системах применяется полный цикл: от сбора требований до вывода из эксплуатации.
- 2) В проектах цифровой трансформации стандарт используется для унификации процессов управления ИТ-ресурсами.

Изм.	Лист	№ докум.	Подпись	Дата	ПП.04.01.09.02.07-009	Лист 13
------	------	----------	---------	------	-----------------------	------------

3) В стартапах применяется укороченная версия жизненного цикла, но с сохранением ключевых принципов архитектурного планирования и сопровождения.

Рекомендации по внедрению стандарта:

1) Необходимо определить, какие процессы являются критически важными для конкретного проекта.

2) Следует адаптировать объем и структуру документации в зависимости от масштаба и типа проекта.

3) Желательно использовать вспомогательные методические материалы, такие как ГОСТ Р ИСО/МЭК ТО 15271.

4) Важно проводить регулярный аудит процессов и корректировать их при изменении проектных условий.

Таким образом, ГОСТ Р ИСО/МЭК 12207 представляет собой универсальный инструмент для управления проектами в области информационных технологий. Его грамотное применение позволяет структурировать деятельность, повысить качество продукта и обеспечить устойчивость проекта к внешним изменениям.

Изм.	Лист	№ докум.	Подпись	Дата	ПП.04.01.09.02.07-009	Лист 14

## **2 Производственный этап**

### **2.1 Участвовать в документировании процессов инсталляции, настройки, обслуживания ПО и результатов мониторинга эксплуатационных характеристик**

Документирование процессов работы с программным обеспечением и результатов его мониторинга является ключевым элементом эффективного управления ИТ-инфраструктурой. Систематическая фиксация действий и показателей обеспечивает воспроизводимость результатов, упрощает аудит, ускоряет устранение неисправностей и формирует корпоративную базу знаний. Качественная документация снижает зависимость от конкретных специалистов и обеспечивает преемственность процессов.

Важные аспекты документирования:

- 1) Разработка и актуализация инструкций по установке и настройке ПО:
  - Создание пошаговых руководств (чек-листов) для инсталляции типового и специализированного ПО с учетом требований безопасности.
  - Фиксация всех выполненных настроек (параметры конфигурационных файлов, реестра, переменные среды).
  - Включение скриншотов ключевых этапов и предупреждений о типичных ошибках.
  - Регулярное обновление инструкций при смене версий ПО или инфраструктуры.

Изм.	Лист	№ докум.	Подпись	Дата	ПП.04.01.09.02.07-009	Лист
						15

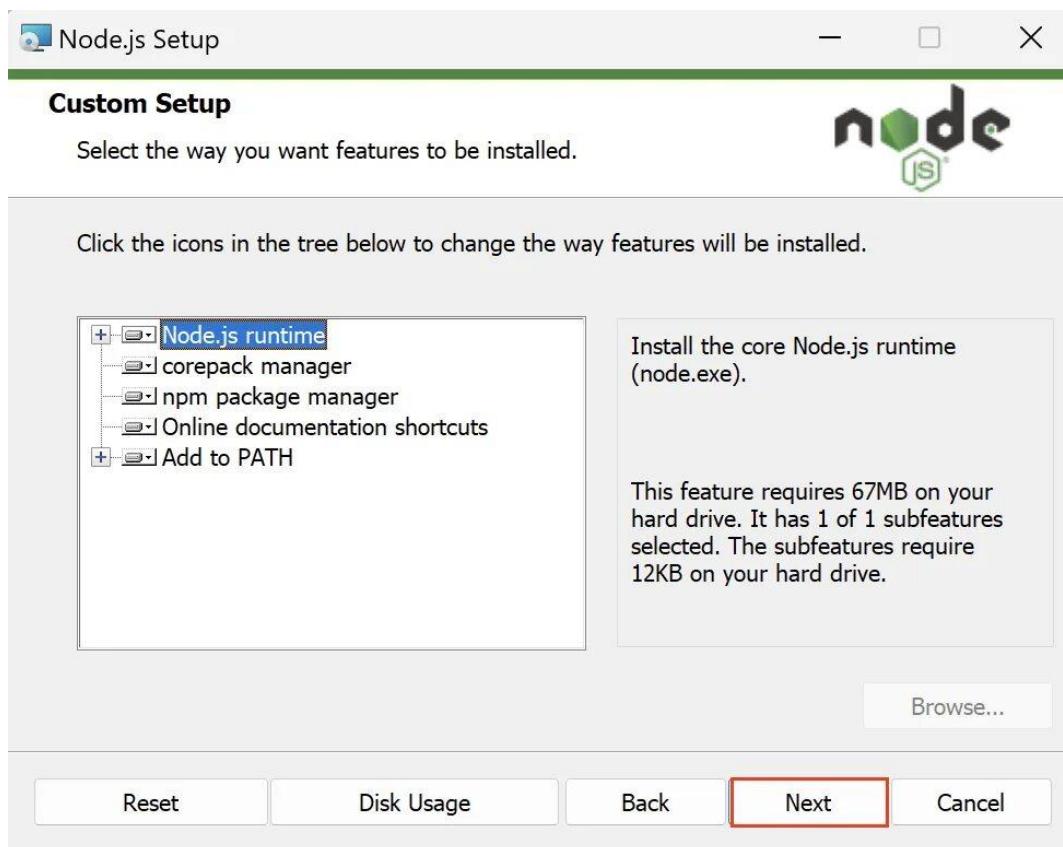


Рисунок 2 – Фрагмент по установке специализированного ПО с указанием критических параметров конфигурации

- 2) Ведение журналов обслуживания и изменений (Change Log):
  - Регистрация всех выполненных операций обслуживания (обновления, патчи, очистка, резервное копирование) с указанием даты, времени и исполнителя.
  - Фиксация причин изменений и их ожидаемого эффекта.
  - Документирование откатов изменений в случае возникновения проблем.
- 3) Формирование отчетов по результатам мониторинга:
  - Систематизация данных мониторинга (графики загрузки ЦП/памяти/диска из Zabbix, PRTG, штатных средств ОС).
  - Анализ тенденций и аномалий в отчетном периоде (неделя/месяц/квартал).

Изм.	Лист	№ докум.	Подпись	Дата

– Представление данных в наглядном виде (диаграммы, сводные таблицы) с выводами.

– Сравнение показателей «до» и «после» внедрения изменений.

4) Ведение реестра (инвентаризации) программного обеспечения и лицензий:

– Поддержание актуального списка установленного ПО на всех управляемых системах.

– Контроль соответствия используемого ПО имеющимся лицензиям.

– Фиксация ключей активации и сроков действия лицензий.

5) Пополнение базы знаний (Knowledge Base) на основе инцидентов:

– Анализ зафиксированных инцидентов (из пункта о поддержке пользователей) и описание решений.

– Создание статей базы знаний с шагами по устранению распространенных проблем.

– Организация информации для удобного поиска (теги, категории).

Документирование процессов и результатов работы с программным обеспечением имеет важное значение по следующим причинам:

1) Наличие четких и актуальных инструкций обеспечивает единообразие установки и настройки программного обеспечения различными специалистами, что уменьшает вероятность ошибок.

2) Документация позволяет быстрее диагностировать и устранять проблемы, поскольку журналы изменений помогают выявить причины сбоев и нештатного поведения системы.

3) Фиксация всех действий в ИТ-инфраструктуре делает процессы прозрачными и позволяет соответствовать требованиям безопасности, в том числе стандарту ГОСТ Р ИСО/МЭК 27001.

4) Анализ данных мониторинга, оформленный в виде отчетов, предоставляет объективную информацию для планирования модернизации, распределения ресурсов или изменения конфигураций.

Иzm.	Лист	№ докум.	Подпись	Дата
------	------	----------	---------	------

5) Документация минимизирует зависимость от конкретных сотрудников, предотвращает потерю важной информации и облегчает адаптацию новых специалистов.

6) Подробная фиксация настроек программного обеспечения, контроль использования лицензий и учет критических параметров позволяют усилить защиту ИТ-инфраструктуры.

## **2.2 Диагностировать проблемы производительности и безопасности программного обеспечения компьютерных систем и участвовать в их оптимизации**

Диагностика проблем производительности и безопасности программного обеспечения является важным этапом в обеспечении стабильной и защищенной работы ИТ-инфраструктуры. Этот процесс включает выявление узких мест, анализ уязвимостей и внедрение решений для оптимизации работы систем. Регулярный мониторинг и своевременное устранение проблем позволяют предотвратить серьезные сбои, повысить эффективность работы и обеспечить безопасность данных.

Важные аспекты диагностики:

- 1) Мониторинг и сбор данных о производительности:
  - Использование специализированных инструментов (например, AIDA64, HWMonitor, Task Manager, Zabbix) для отслеживания ключевых показателей: загрузка ЦП, использование памяти, температура компонентов, скорость дисковых операций.
  - Фиксация аномалий (например, перегрев процессора, утечки памяти, высокая загрузка диска) и их корреляция с жалобами пользователей.
  - Анализ журналов событий (Event Viewer, системные логи) для выявления ошибок и предупреждений.

Изм.	Лист	№ докум.	Подпись	Дата

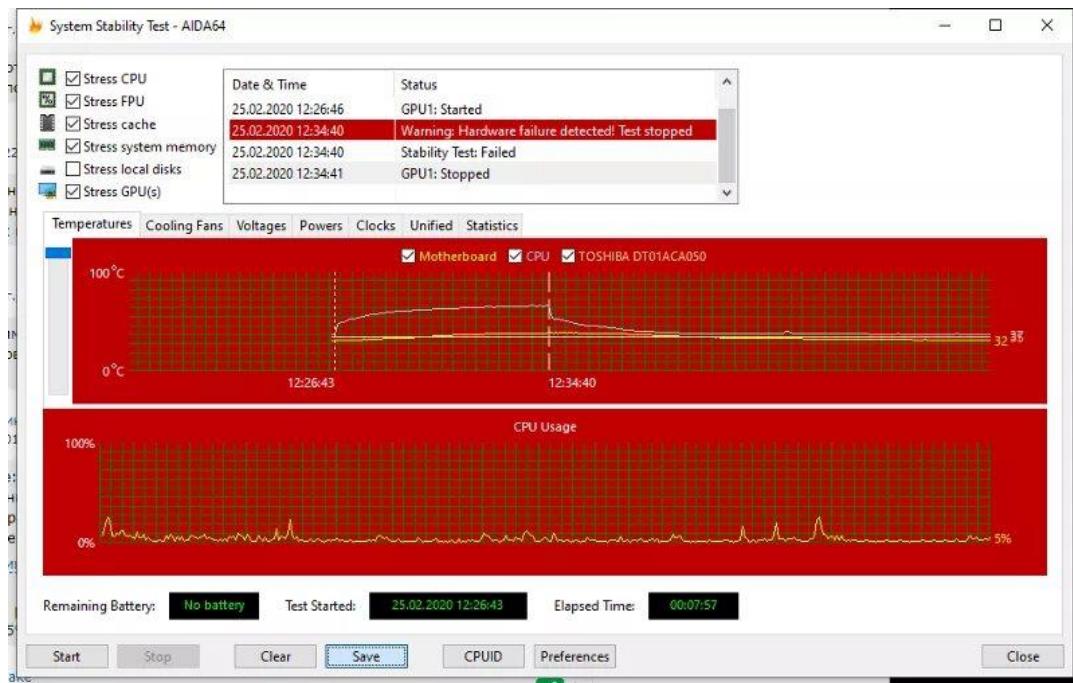


Рисунок 3 – Скриншот мониторинга системы с показателями температуры, загрузки ЦП и памяти, используемый для диагностики проблем производительности

- 2) Выявление узких мест и причин снижения производительности:
    - Определение процессов или служб, потребляющих чрезмерные ресурсы (например, фоновые приложения, вирусы, некорректные драйверы).
    - Проверка состояния оборудования (износ дисков, перегрев, недостаточное охлаждение).
    - Анализ сетевой задержки (если ПО работает в распределенной среде).
  - 3) Диагностика уязвимостей и проблем безопасности:
    - Проверка актуальности обновлений ОС и ПО (включая патчи безопасности).
    - Анализ настроек безопасности (брандмауэр, права доступа, шифрование данных).
    - Использование сканеров уязвимостей (например, Nessus, OpenVAS)
- для выявления потенциальных угроз.

Изм.	Лист	№ докум.	Подпись	Дата

4) Оптимизация производительности и устранение проблем:

- Настройка параметров ОС (например, отключение ненужных служб, оптимизация автозагрузки, настройка файла подкачки).
- Обновление драйверов и прошивок оборудования.
- Внедрение рекомендаций по улучшению (например, добавление оперативной памяти, переход на SSD, настройка балансировки нагрузки).

5) Тестирование и оценка результатов оптимизации:

- Сравнение показателей производительности до и после внесения изменений.
- Проведение нагрузочного тестирования (например, с помощью JMeter) для проверки стабильности системы.
- Фиксация результатов в отчетах для дальнейшего анализа.

Диагностика производительности и безопасности программного обеспечения играет ключевую роль в поддержании стабильной и эффективной работы ИТ-систем. Она важна по следующим причинам:

- 1) Раннее обнаружение проблем, таких как перегрев, утечки памяти или уязвимости, помогает избежать критических отказов и длительных простоев.
- 2) Оптимизация использования ресурсов, устранение «узких мест» и настройка системы увеличивают скорость работы приложений и снижают нагрузку на оборудование.
- 3) Своевременное выявление и устранение уязвимостей защищает данные от несанкционированного доступа, вредоносных программ и кибератак.
- 4) Оптимизация параметров работы программного и аппаратного обеспечения продлевает срок службы оборудования и снижает необходимость его преждевременной замены.
- 5) Стабильная и быстрая работа программного обеспечения улучшает опыт пользователей и способствует росту производительности сотрудников.

Изм.	Лист	№ докум.	Подпись	Дата
------	------	----------	---------	------

6) Проведение регулярного анализа производительности и безопасности помогает соблюдать стандарты и законодательства в области защиты информации, такие как GDPR или ФЗ-152.

## **2.3 Оказывать техническую поддержку пользователям и устранять неисправности в работе программного обеспечения компьютерных систем**

Оказание технической поддержки пользователям и оперативное устранение неисправностей ПО являются критически важными функциями для обеспечения бесперебойной работы любого предприятия. Этот процесс напрямую влияет на производительность труда сотрудников и минимизацию простоев, вызванных техническими проблемами. Эффективная поддержка требует не только знаний ПО, но и умения быстро диагностировать проблемы, используя доступные инструменты и данные.

Важные аспекты технической поддержки пользователей:

1) Диагностика проблем на основе жалоб пользователей и данных мониторинга:

– Активное взаимодействие с пользователями для понимания сути проблемы (описание симптомов, условия возникновения).

– Использование данных системного мониторинга (как на рисунке 4) для объективной оценки состояния системы (температуры ЦП/чипсета, напряжения, загрузки памяти, скорости вентиляторов).

– Сопоставление субъективных жалоб пользователей (например, «компьютер тормозит», «программа зависает») с объективными показателями ресурсов для выявления корневой причины (перегрев, нехватка памяти, сбойный процесс).

Изм.	Лист	№ докум.	Подпись	Дата	ПП.04.01.09.02.07-009	Лист
						21

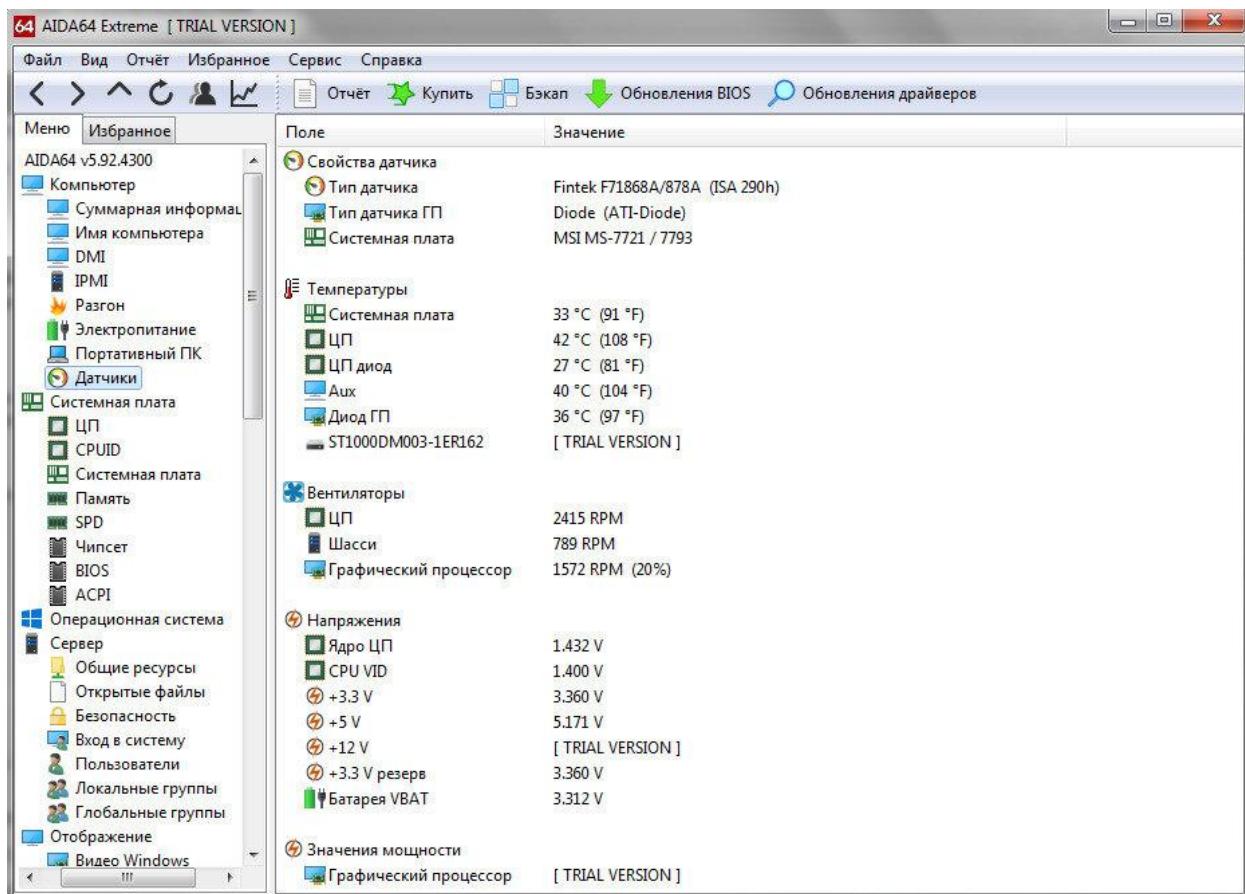


Рисунок 4 – Скриншот утилиты мониторинга (AIDA64) с показателями ресурсов системы - используется для диагностики причин нестабильной работы ПО

- 2) Применение стандартных процедур устранения неисправностей:
  - Следование внутренним регламентам и чек-листам для решения типовых проблем (перезапуск служб, очистка кэша, проверка обновлений, восстановление системы).
  - Выполнение точечной переустановки или восстановления поврежденных компонентов ПО.
  - Настройка параметров операционной системы и приложений для разрешения конфликтов или оптимизации работы под конкретную конфигурацию оборудования (например, настройка электропитания при перегреве, видимом на рис. 4).

- 3) Работа с системами учета инцидентов (Ticketing Systems) и документирование:

Изм.	Лист	№ докум.	Подпись	Дата	ПП.04.01.09.02.07-009	Лист
						22

- Регистрация всех обращений пользователей и предпринятых действий в специализированной системе (например, Jira Service Desk, Zendesk).
- Четкое описание симптомов, проведенной диагностики, выполненных шагов по устранению и конечного результата.
- Обновление внутренней базы знаний (Knowledge Base) на основе решенных инцидентов для ускорения решения аналогичных проблем в будущем.

4) Коммуникация и обучение пользователей:

- Предоставление пользователям понятных инструкций и консультаций по использованию ПО.
- Информирование пользователя о статусе решения его проблемы.
- Проведение кратких инструктажей или создание памяток для предотвращения повторения распространенных ошибок, вызванных действиями пользователя.

5) Эскалация сложных проблем:

- Своевременное определение проблем, требующих вмешательства более опытных специалистов (системных администраторов, разработчиков).
- Грамотная передача инцидента с полной информацией о диагностике и предпринятых действиях для ускорения решения.

Оперативная и качественная техническая поддержка пользователей необходима для стабильной работы программного обеспечения и всей ИТ-инфраструктуры. Она имеет важное значение по следующим причинам:

- 1) Быстрое реагирование на технические проблемы и их эффективное устранение позволяют обеспечить непрерывность бизнес-процессов и поддерживать высокую производительность сотрудников.
- 2) Своевременная помощь, вежливое взаимодействие и доступные объяснения создают положительный пользовательский опыт и укрепляют доверие к ИТ-подразделению.

Изм.	Лист	№ докум.	Подпись	Дата
------	------	----------	---------	------

3) Раннее выявление неисправностей, таких как перегрев или перегрузка ресурсов (например, зафиксированных при мониторинге, как на рисунке 4), позволяет устраниить причины сбоев до того, как они приведут к отказу оборудования или программ.

4) Решение типовых проблем на первом уровне технической поддержки снижает нагрузку на более квалифицированных специалистов и уменьшает необходимость в привлечении внешних ресурсов.

5) Регулярное документирование инцидентов и способов их решения формирует внутреннюю базу знаний, что ускоряет устранение повторяющихся проблем и облегчает обучение новых сотрудников.

6) Своевременное реагирование на инциденты, связанные с уязвимостями программного обеспечения или подозрительной активностью, помогает предотвратить потенциальные угрозы и защищает корпоративные данные.

Изм.	Лист	№ докум.	Подпись	Дата
------	------	----------	---------	------

## ЗАКЛЮЧЕНИЕ

Практическое знакомство с различными моделями оценки качества программного обеспечения, а также с процессами его установки, конфигурации и технического обслуживания позволило получить ценные профессиональные инсайты. Особое значение приобрело понимание фундаментальной роли качества ПО в современных цифровых системах. Каждая из рассмотренных методологий демонстрирует особый взгляд на проблему обеспечения и измерения качества, предоставляя эффективные инструменты для его постоянного совершенствования, что напрямую влияет на пользовательскую удовлетворенность и минимизирует потенциальные риски, связанные с программными сбоями.

Не менее важным оказался аспект соблюдения норм безопасности труда, который наглядно продемонстрировал прямую зависимость между комфорtnыми условиями работы и производительностью персонала. Практические навыки по развертыванию и поддержке программных решений убедительно доказали, что грамотная первоначальная настройка и систематическое обслуживание являются обязательными условиями стабильной и эффективной работы ИТ-инфраструктуры.

Полученный опыт значительно углубил понимание принципов обеспечения качества программных продуктов и на практике подтвердил, что использование качественного ПО служит надежной основой для достижения выдающихся результатов как на индивидуальном уровне, так и в рамках коллективной работы над проектами.

Изм.	Лист	№ докум.	Подпись	Дата	ПП.04.01.09.02.07-009	Лист 25
------	------	----------	---------	------	-----------------------	------------

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Об информации, информационных технологиях и о защите информации: Федеральный закон № 149-ФЗ от 27.07.2006 (ред. от 02.07.2021). - М.: Проспект, 2021. - 32 с.
2. О персональных данных: Федеральный закон № 152-ФЗ от 27.07.2006 (ред. от 24.02.2021). – М.: Проспект, 2021. - 48 с.
3. О безопасности критической информационной инфраструктуры РФ: Федеральный закон № 187-ФЗ от 26.07.2017 (ред. от 02.07.2021). - М.: Проспект, 2021. - 56 с.
4. О коммерческой тайне: Федеральный закон № 98-ФЗ от 29.07.2004 (ред. от 09.03.2021). - М.; Проспект, 2021. - 40 с.
5. ГОСТ Р 56939-2016. Защита информации. Средства вычислительной техники. Требования к средствам высоконадежной биометрической аутентификации. - М.: Стандартинформ, 2016. - 28 с.
6. ГОСТ Р 57580.1-2017. Безопасность финансовых организаций. Требования к защите информации. - М.: Стандартинформ, 2017. - 36 с.
7. ГОСТ Р ИСО/МЭК 15408-2013. Информационная технология. Методы и средства обеспечения безопасности. - М.: Стандартинформ, 2013. - 112 с.
8. Инструкция по охране труда при работе на персональных компьютерах в ПАО «Ростелеком»: утв. приказом 01/01/482/23 от 2023 г. - 15 с.
9. Об утверждении требований по защите информации в государственных информационных системах: Приказ ФСТЭК России №21 от 11.02.2013. - 24 с.
10. Барский, А.Б. Компьютерные сети и технологии / А.Б. Барский. - М.: Академия, 2019. - 384 с. - ISBN 978-5-4468-5678-9.
11. Вишневский, В.М. Теоретические основы проектирования компьютерных сетей / В.М. Вишневский. - М.: Техносфера, 2018. - 512 с. - ISBN 978-5-94836-512-3.

Изм.	Лист	№ докум.	Подпись	Дата	ПП.04.01.09.02.07-009	Лист
						26

12. Галатенко, В.А. Основы информационной безопасности / В.А. Галатенко. - М.: Интернет-Университет, 2020. - 280 с. - ISBN 978-5-9556-0421-5.
13. Гук, М.Ю. Аппаратные средства локальных сетей / М.Ю. Гук. - СПб.: Питер, 2020. - 576 с. - ISBN 978-5-4461-1123-5.
14. Дейтел, Х.Дж. Операционные системы / Х.Дж. Дейтел, П.Дж. Дейтел. - М.: Бином, 2017. - 1120 с. - ISBN 978-5-9518-0241-4.
15. Золотарёв, В.В. Защита информации в компьютерных системах / В.В. Золотарёв. - М.: Форум, 2019. - 368 с. - ISBN 978-5-00091-567-1.
16. Касперски, К. Техника оптимизации программ / К. Касперски. - СПб.: БХВ-Петербург, 2018. - 464 с. - ISBN 978-5-9775-3963-8.
17. Корнеев, И.К. Защита информации в компьютерных системах и сетях / И.К. Корнеев. - М.: Радио и связь, 2019. - 344 с. - ISBN 978-5-256-02456-7.
18. Кузьмин, А.С. Современные операционные системы / А.С. Кузьмин. - М.: Солон-Пресс, 2020. - 416 с. - ISBN 978-5-91359-312-7.
19. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы / В.Г. Олифер, Н.А. Олифер. - СПб.: Питер, 2021. - 992 с. - ISBN 978-5-4461-1456-4.
20. Партика, Т.Л. Защита информации в компьютерных системах / Т.Л. Партика, И.И. Попов. - М.: Форум, 2018. - 432 с. - ISBN 978-5-00091-512-1.
21. Росляков, А.В. Криптографические методы защиты информации / А.В. Росляков. - М.: Горячая линия - Телеком, 2020. - 288 с. - ISBN 978-5-9912-0721-3.
22. Таненбаум, Э. Современные операционные системы / Э. Таненбаум. - СПб.: Питер, 2019. - 1120 с. - ISBN 978-5-4461-1156-3.
23. Фёдоров, А.Г. Администрирование локальных сетей / А.Г. Фёдоров. - М.: ДМК Пресс, 2020. - 480 с. - ISBN 978-5-97060-789-5.

Изм.	Лист	№ докум.	Подпись	Дата

ПП.04.01.09.02.07-009

Лист

27

24. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей / В.Ф. Шаньгин. - М.: Форум, 2019. - 416 с. - ISBN 978-5-00091-589-3.

25. Якубов, А.С. Оптимизация и настройка ПК для максимальной производительности / А.С. Якубов. - СПб.: БХВ-Петербург, 2021. - 320 с. - ISBN 978-5-9775-6745-7.

Изм.	Лист	№ докум.	Подпись	Дата	ПП.04.01.09.02.07-009	Лист 28