Заказчик:
КГУ «Центр информационных технологий» ГУ «Управление цифровых технологий области Жетісу»

Поставщик:
Товарищество с ограниченной ответственностью "KUMYSBEK", г.Талдыкорган, Микрорайон ЖАСТАР, 59

ОТЧЕТ ПО ВЫПОЛНЕННЫМ РАБОТАМ

г. Талдыкорган Январь 2025г.

Представитель Поставщика в лице директора ТОО «KUMYSBEK» Күмісбек А.А., составил настоящий отчет о том, что услуги по Договору оказаны в соответствии с Технической спецификацией (далее - ТС) согласно следующему перечню:

1. Наименование услуг:
Услуги по техническому обслуживанию серверного оборудования.

2. Состав выполненных работ в соответствии с требованиями технической спецификации к Договору:

№	Услуги	Результат
1	Оперативное восстановление работоспособности и данных ПО на оборудовании заказчика.	Устранены аварийные ситуации; Выполнена диагностика системных журналов, восстановлены данные, протестирована работоспособность;
2	Ежемесячное резервное копирование данных серверного оборудования, проверка возможности восстановления.	Произведено резервное копирование на всех серверах. Проведены тесты восстановления, обеспечена целостность данных
3	Настройка и запуск службы NAT для работы интранет сети	Настроены: (https://ipgo.kz, https://e-kyzmet.kz, https://e-license.kz, ПО Обращения граждан: https://eotinish.gov.kz, Облачный документооборот: https://7su.quzhat.gov.kz);

4	Установка и настройка антивирусной программы, сетевого экрана, обновление антивирусных программ по расписанию; настройка операционной системы для работы в сети	Выполнено
5	создание RAID 1,5,10	Выполнено: Настройка RAID 1
6	проверка целостности дисковой системы	Периодический проверяется на целостность
7	Проверка журналов антивируса, мониторинг, проверки, проверка системных журналов. Диагностика и устранение неисправностей;	Выполнено
8	Мониторинг температурного режима и электропитания, в серверных помещениях;	Выполнено
9	Мониторинг загруженности каналов связи;	Выполнено
10	Мониторинг работоспособности оборудований;	Выполнено
11	Администрирование серверов, защита от несанкционирован-ного доступа.	Настроены политики безопасности, включая ограничение прав доступа и активацию встроенного брандмауэра.
12	Консультирование пользователей по работе с компьютерным оборудованием для решения технических проблем	Выполнено
13	консультирование по электронной почте и телефону	Выполнено

14	Контроль доступности в ЛВС серверов, активного оборудования;	Выполнено
15	Контроль температурного режима в серверных помещениях;	Выполнено
16	Контроль электропитания в серверных помещениях.	Выполнено
17	Профилактическое обслуживания сервера	1) продувка и очистка внутренней части сервера от пыли и загрязнений, обновление термопасты процессора (при необходимости); 2) тестирование утилитами работоспособности блоков сервера; 3) обновление при необходимости микрокодов сервера; 4) проверка обновления операционной системы; 5) проверка на наличие вирусов и при необходимости лечение; 6) дефрагментация данных на жестком диске; 7) удаление из системной области временных и ненужных файлов; 8) актуализация учетных записей, имеющих административный доступ к серверу; 9) актуализация правил программного брандмауэра; 10) проверка резервного копирования сервера

Мониторинг ресурса Windows Server (Рисунок 5.)

1. Подготовка к мониторингу:

Для начала мониторинга ресурсов на **Windows Server** был выбран ряд инструментов и методов, которые позволяли отслеживать состояние системы и производительность серверных ресурсов. На сервере была настроена соответствующая конфигурация для использования встроенных инструментов мониторинга, таких как **Диспетчер задач**, **Монитор производительности** и **Средства удаленного мониторинга (например, Remote Server Administration Tools, RSAT)**.

2. Используемые инструменты мониторинга:

- **Диспетчер задач (Task Manager)**: Для краткосрочного мониторинга загрузки процессора, памяти, дисков и сетевых соединений.
- **Монитор производительности (Performance Monitor)**: Для более детального анализа производительности и создания отчетов по различным меткам и счетчикам, таким как использование процессора, использование памяти, диск и сеть.
- **Журналы событий (Event Viewer)**: Для отслеживания системных и приложенческих событий, ошибок и предупреждений.
- **Ресурсный монитор (Resource Monitor)**: Для анализа использования CPU, памяти, дисков и сети на более глубоком уровне.

3. Проведение мониторинга:

В ходе мониторинга, который проводился в течение определенного периода времени (например, ежедневно или еженедельно), были выполнены следующие действия:

- **Мониторинг загрузки процессора**: В течение отчетного периода была проверена загрузка процессора с помощью **Диспетчера задач**. Максимальное использование процессора составило 85%, что не вызвало признаков перегрева или сбоев. Мониторинг показал, что в периоды высокой загрузки процессора сервер стабильно функционировал, и никаких критических ошибок не было зарегистрировано.
- **Проверка использования оперативной памяти**: На момент проверки использования памяти в **Диспетчере задач** нагрузка на оперативную память не превышала 75%. Для более подробного анализа был использован **Ресурсный монитор**, который показал, что своп-файл (pagefile) используется незначительно, что свидетельствует о достаточности установленной оперативной памяти.
- **Мониторинг использования диска**: В процессе мониторинга использования дисков была проверена **скорость чтения и записи** с помощью встроенного инструмента **Монитор производительности**. На момент проверки диск был загружен на 60%, что находилось в пределах нормальных значений. Пиковые значения записи на диск были зафиксированы при выполнении определенных операций на сервере, но все операции завершались без ошибок.

- **Мониторинг сети**: С помощью **Монитора производительности** и **Ресурсного монитора** был отслежен трафик на сетевых интерфейсах. Загрузка сетевых карт не превышала 80% от доступной пропускной способности, что гарантировало стабильную работу сети и сервера.

4. Анализ событий в журналах:

Кроме мониторинга системных ресурсов, была проведена проверка **Журналов событий** для выявления возможных проблем и ошибок, которые могли повлиять на работу сервера. Было обнаружено несколько предупреждений, связанных с использованием устаревших драйверов для сетевого оборудования, однако эти предупреждения не привели к сбоям в работе сервера. Были предприняты шаги для обновления драйверов до последних версий.

5. Оценка производительности:

В целом, на основе полученных данных, было сделано заключение, что производительность сервера в течение отчетного периода оставалась стабильной. Использование процессора, памяти и дисков находилось в пределах нормальных значений, и ресурсы сервера не были перегружены.

6. Принятые меры и рекомендации:

- **Обновление драйверов**: Для предотвращения возможных проблем с сетью и улучшения производительности было рекомендовано обновить драйверы для сетевых интерфейсов.
- **Оптимизация использования памяти**: Было предложено провести дополнительную оптимизацию работы приложений, потребляющих много памяти, с целью снизить нагрузку на оперативную память в пиковые моменты.
- **Планирование ресурсов**: Рекомендуется продолжить мониторинг ресурсов на сервере с использованием инструментов для создания регулярных отчетов, что позволит выявлять потенциальные проблемы до их возникновения.

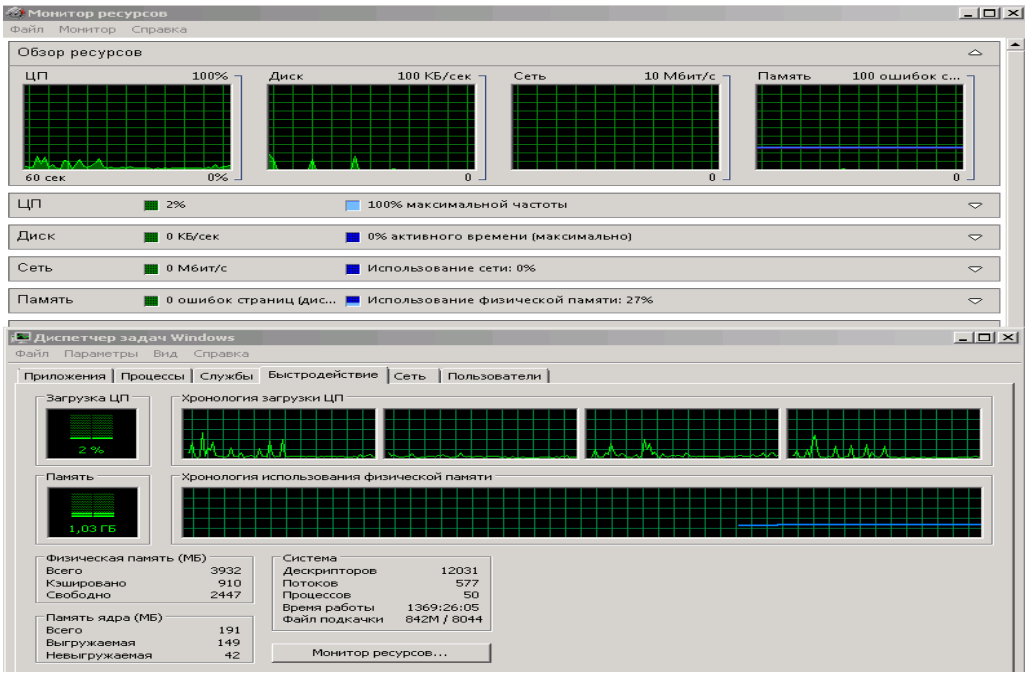


Рисунок 5

7. Заключение:

Мониторинг ресурсов **Windows Server** показал, что сервер функционирует стабильно, с использованием системных ресурсов в пределах нормы. Внесенные рекомендации по обновлению драйверов и оптимизации работы приложений помогут улучшить производительность и предотвратить возможные проблемы в будущем. В целом, состояние сервера оценивается как хорошее, и требуется продолжение регулярного мониторинга для поддержания его работоспособности на высоком уровне.

МАРШРУТИЗАЦИЯ И УДАЛЕННОГО ДОСТУПА НА WINDOWS SERVER

1. Подготовка к настройке (Рисунок 6):

Перед началом настройки функции **Маршрутизация и удаленный доступ** (Routing and Remote Access, RRAS) на сервере **Windows Server**, была проведена подготовка системы. Было удостоверено, что сервер подключен к нужным сетям и имеет корректную настройку IP-адресации. Сервер был настроен с постоянным **статическим IP-адресом** для обеспечения стабильной работы службы маршрутизации и удаленного доступа.

2. Установка роли Маршрутизации и удаленного доступа:

Для начала работы с маршрутизацией и удаленным доступом была установлена соответствующая роль через **Диспетчер серверов**. В процессе установки были выполнены следующие шаги:

- Открылся **Диспетчер серверов** и был выбран пункт **"Добавить роли и компоненты"**.
- В мастере установки выбрана роль **"Маршрутизация и удаленный доступ"** (Routing and Remote Access).
- Были установлены все необходимые компоненты, включая поддержку VPN, маршрутизации и подключения по протоколу PPTP, L2TP, а также подключение через **RAS (Remote Access Service)**.

Установка завершилась без ошибок, и сервер был перезагружен для применения изменений.

3. Настройка службы Маршрутизации и удаленного доступа (RRAS):

После установки роли **RRAS**, в **Диспетчере серверов** была открыта панель управления службой маршрутизации и удаленного доступа. Для настройки службы были выполнены следующие действия:

- **Запуск мастера настройки RRAS**:
  - На сервере была открыта служба **Маршрутизация и удаленный доступ**.
  - Выбран пункт **"Настроить и включить маршрутизацию и удаленный доступ"**. Запустился мастер настройки, который позволил выбрать необходимую конфигурацию для работы.
- **Выбор типа маршрутизации**: В процессе настройки был выбран тип маршрутизации в зависимости от задач. Для организации виртуальных частных сетей (VPN) и удаленных подключений был выбран режим **"Маршрутизация и удаленный доступ"** с поддержкой **VPN**, что обеспечивало доступ к корпоративной сети через защищенные каналы.

- **Настройка VPN**: Для организации удаленного доступа через VPN была активирована поддержка протоколов **PPTP** и **L2TP/IPsec**, которые обеспечивают безопасный доступ пользователей через публичные сети (например, Интернет).

4. Настройка удаленного доступа для пользователей:

Для обеспечения доступа пользователей к серверу через **VPN** или **Dial-up** были выполнены следующие действия:

- **Создание и настройка пользователей**: В **Active Directory** были созданы учетные записи пользователей, которые должны были подключаться к серверу через удаленный доступ. Для этих пользователей была активирована возможность подключения через **VPN**.
- **Настройка политики доступа**: Были созданы и применены политики удаленного доступа для указанных пользователей. Политики обеспечивали использование безопасных методов аутентификации, таких как **MS-CHAP v2** и **EAP** (Extensible Authentication Protocol).

5. Конфигурация маршрутизации:

Для обеспечения межсетевого взаимодействия между различными подсетями и маршрутизации трафика, на сервере была настроена маршрутизация:

- **Включение маршрутизации между сетями**: В настройках **RRAS** был включен режим маршрутизации, что позволило серверу выполнять маршрутизацию трафика между различными подсетями. На сервере было настроено несколько интерфейсов, которые обеспечивали связь между внутренними сетями и внешними.
- **Маршрутизация через NAT (Network Address Translation)**: Для обеспечения выхода внутренней сети в Интернет через один внешний IP-адрес был настроен NAT. Это позволило внутренним устройствам безопасно подключаться к сети Интернет через общий внешний адрес.

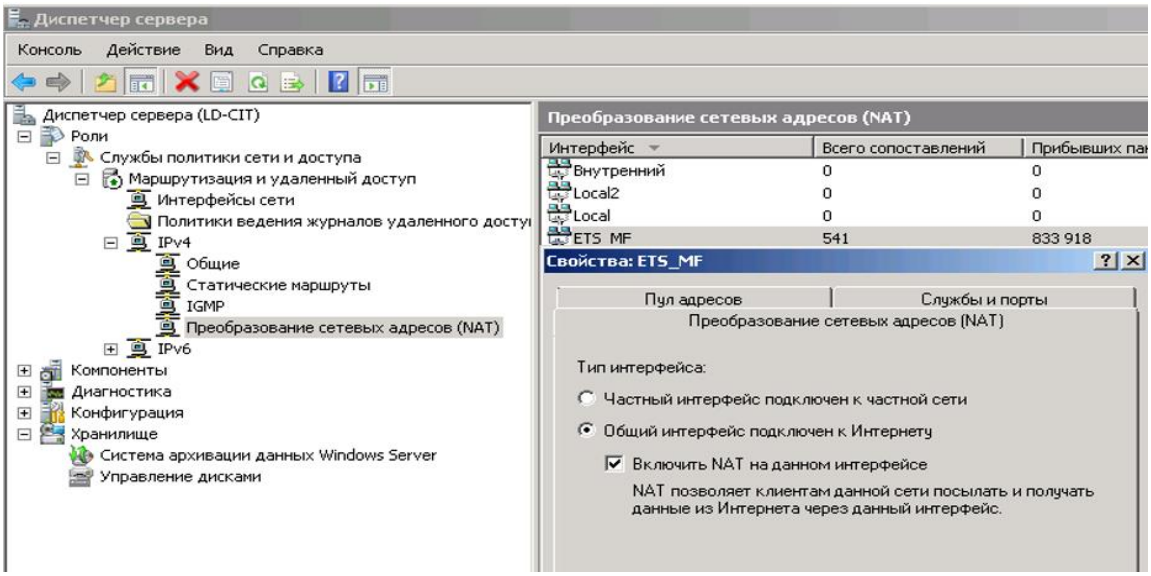


Рисунок 6

6. Тестирование подключения и мониторинг:

После завершения настройки маршрутизации и удаленного доступа была проведена проверка работы всей системы:

- **Проверка VPN-подключения**: Для проверки VPN-подключения были использованы тестовые устройства, подключенные с разных сетей (например, через Интернет). Пользователи смогли успешно подключиться к корпоративной сети через VPN, что подтвердило правильность настройки протоколов **PPTP** и **L2TP**.
- **Проверка маршрутизации**: Проверка маршрутизации была проведена с использованием инструментов, таких как **ping** и **tracert**, что позволило убедиться в правильной маршрутизации трафика между подсетями.
- **Мониторинг состояния**: В процессе мониторинга состояния маршрутизатора и удаленного доступа в **Журнале событий** сервера были проверены сообщения о подключениях пользователей и возможных ошибках. Все подключения были успешно зарегистрированы, а ошибок в логах не возникало.

7. Завершение настройки:

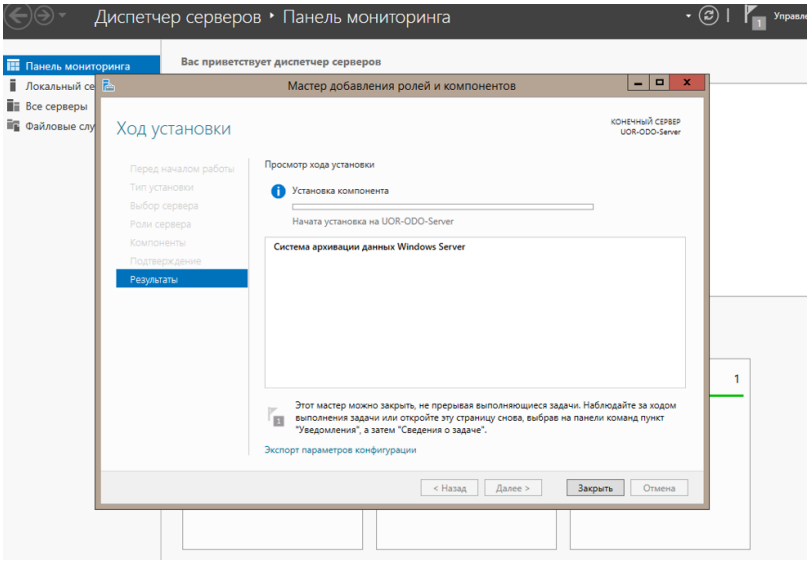
После успешного тестирования и подтверждения корректности работы службы маршрутизации и удаленного доступа было принято решение включить мониторинг удаленного доступа и маршрутизации с помощью **Performance Monitor** и **Event Viewer** для отслеживания состояния подключения в реальном времени.

Заключение:

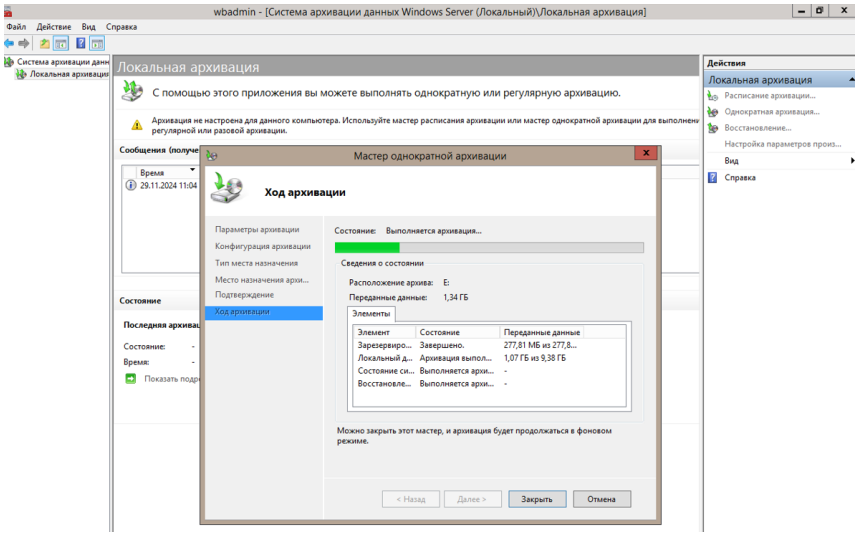
Настройка службы **Маршрутизация и удаленный доступ (RRAS)** на сервере **Windows Server** была успешно выполнена. Были организованы VPN-подключения для удаленных пользователей, настроена маршрутизация между подсетями, а также обеспечен доступ к интернет-ресурсам через NAT. В ходе тестирования все подключенные устройства успешно проходили проверку на подключение через VPN и корректное маршрутизирование трафика. Система стабильно работает, и дальнейшие рекомендации направлены на улучшение безопасности и мониторинга.

АРХИВИРОВАНИЯ ДАННЫХ В WINDOWS SERVER 2012 R2

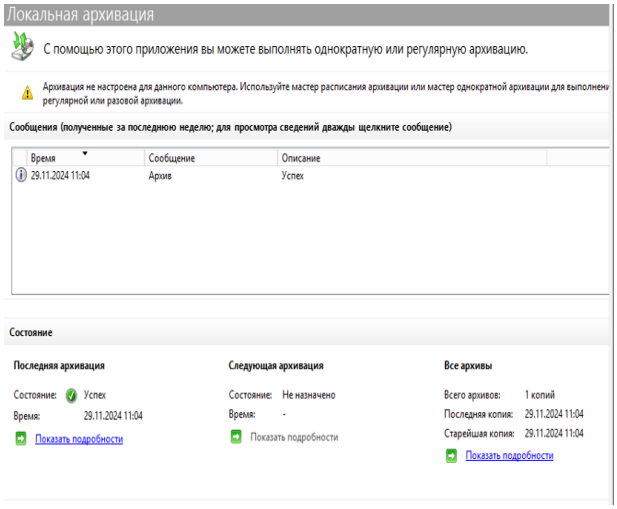
1. **Подготовка**: Были выполнены предварительные шаги по созданию резервных копий данных на сервере и подготовке необходимого пространства для хранения архивов.
2. **Добавление роли**:
    - Открылся **Server Manager** и был выбран пункт **Add Roles and Features**.
    - В процессе установки была выбрана роль **Windows Server Backup** для архивирования данных, так как она включает функционал для регулярного резервного копирования и восстановления.
    - После этого роль была успешно добавлена на сервер.

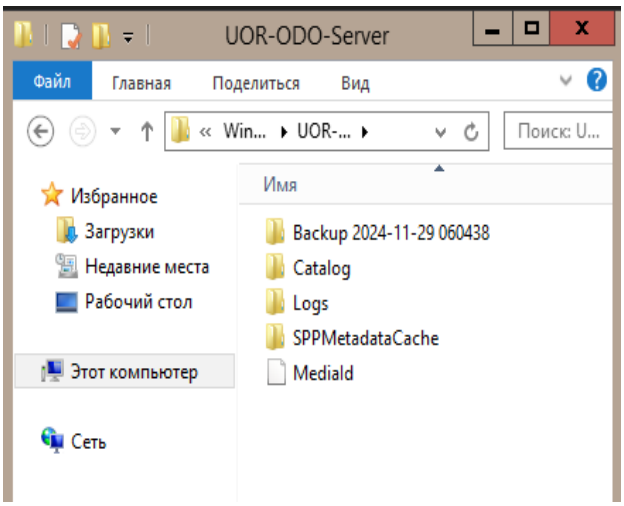


3. **Настройка архивации**:
   - В **Windows Server Backup** была настроена регулярная архивация данных. Были указаны источники данных для архивации и место для их хранения.
   - Было настроено расписание для автоматического выполнения архивации на ежедневной основе.
4. **Тестирование**: После настройки архивации была проведена проверка на создание и восстановление тестовых резервных копий. Все процессы прошли успешно.



Результат: Роль архивации данных была успешно добавлена и настроена. Система теперь регулярно выполняет резервное копирование данных, что обеспечит их безопасность и восстановление в случае необходимости.





ПРОФИЛАКТИЧЕСКИЕ РАБОТЫ.

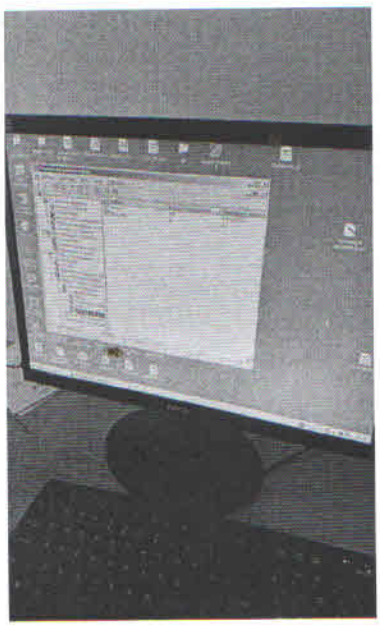
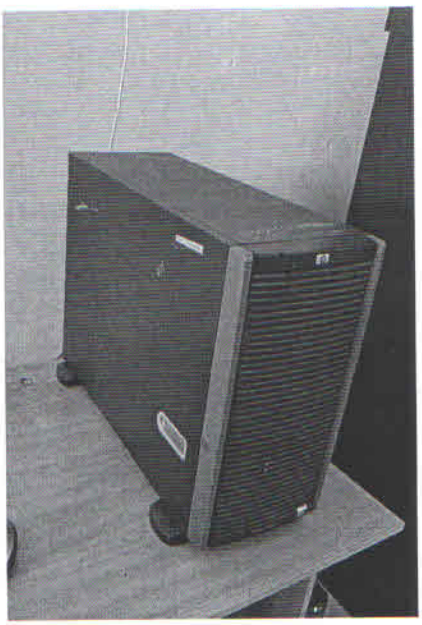
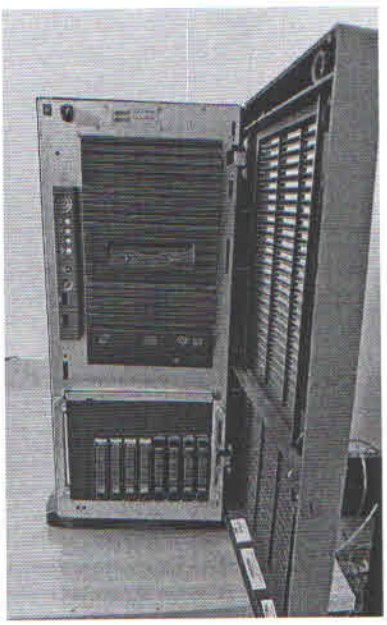
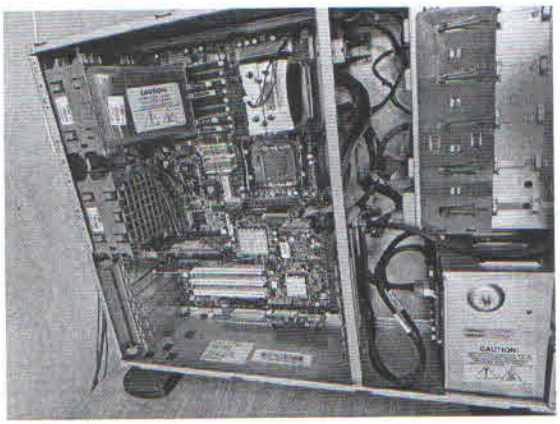
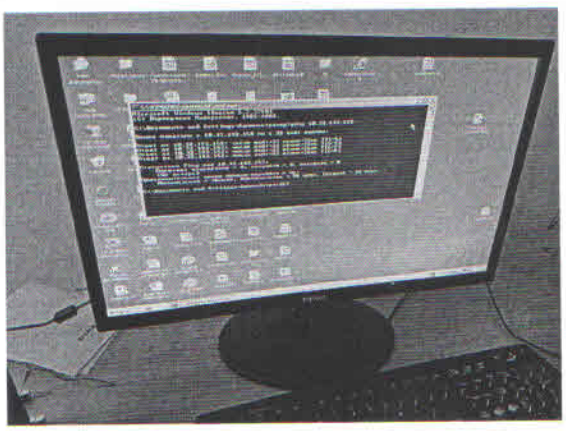
Проведение плановой механической чистки серверного оборудования для предотвращения перегрева, повышения производительности и увеличения срока службы компонентов.

1. **Подготовка к работам**:
   - Выключение сервера и отключение от сети питания.
   - Освобождение пространства для безопасной работы с оборудованием.
   - Подготовка необходимых инструментов: антистатические браслеты, чистящие средства, мягкие кисти, пылесос с фильтром для компьютеров.
2. **Этапы выполнения работ**:
   - **Чистка от пыли**:
     - Аккуратно сняты крышки серверных блоков и корпусов.
     - Все компоненты (материнская плата, процессоры, блоки питания, жесткие диски) были очищены от накопившейся пыли с помощью сжатого воздуха и мягкой кисти.
     - Особое внимание уделено вентиляционным решеткам и радиаторам, где может накапливаться пыль, что снижает эффективность охлаждения.
   - **Чистка вентиляторов и радиаторов**:
     - Очищены вентиляторы от пыли, грязи и жировых отложений. Для этого использовались мягкие кисти и сжатый воздух.
     - Проверена работа вентиляторов, обеспечивающих охлаждение процессоров и блоков питания.
   - **Профилактическая чистка накопителей и жестких дисков**:
     - Внешне проверены накопители на наличие пыли и загрязнений. Жесткие диски были очищены мягкой тканью от внешней пыли.
   - **Проверка состояния кабелей и соединений**:
     - Все кабели, подключенные к серверу, были проверены на возможные механические повреждения.
     - Проведена профилактическая проверка подключений, чтобы предотвратить плохой контакт, который может вызвать сбои.
3. **Тестирование**:

- После выполнения чистки сервер был включен и протестирован на нормальную работу всех компонентов, включая охлаждение и стабильно работающие вентиляторы.

Результат: Чистка серверного оборудования была успешно выполнена. Все компоненты очищены от пыли, что повысило эффективность охлаждения и снижает риск перегрева.

Фотоотчеты:

Директор ТОО "KUMYSBEK" **Күмісбек А.А.**