

## **Авторы:**

Шомахов Ислам Аликович – студент 4 курса Российского государственного университета нефти и газа (Национальный исследовательский университет) имени И.М. Губкина;

Каленский Егор Анатольевич – студент 4 курса Российского государственного университета нефти и газа (Национальный исследовательский университет) имени И.М. Губкина

## **Оценка производительности резервного копирования на базе ОС Альт:**

### **Кибербэкап и UrBackup**

#### **Аннотация**

В данной статье рассматриваются два комплексных решения, которые позволяют работать с резервными копиями в ОС Альт: Кибер Бэкап и UrBackup. Внимание акцентировано на производительности данных продуктов, проводится сравнение скорости и времени их резервного копирования и восстановления данных.

#### **Ключевые слова**

Резервное копирование, КиберБэкап, UrBackup, восстановление данных, производительность, ОС Альт, бэкап.

#### **Введение**

Эффективное управление резервным копированием данных является одной из ключевых задач обеспечения информационной безопасности. В условиях растущего объема информации и необходимости минимизации времени простоя систем, выбор программного обеспечения для создания и восстановления резервных копий становится критически важным. Среди множества доступных решений особое внимание заслуживают инструменты для работы в операционной системе Альт, такие как UrBackup и Кибер Бэкап.

Объектом исследования является процесс резервного копирования и восстановления данных в операционной системе Альт.

Предмет исследования – производительность решений UrBackup и Кибер Бэкап в контексте скорости выполнения операций резервного копирования и восстановления данных.

Цель работы – провести сравнительный анализ указанных инструментов, оценить их эффективность и предложить рекомендации по выбору оптимального решения для использования в инфраструктуре, работающей на ОС Альт.

В настоящее время в Интернет-пространстве существует огромное количество статей и инструкций по развертыванию и администрированию различных проектов по резервному копированию данных. Например, на сайте Хабра имеется статья автора Алексея Федорова (@CyberAGF) [3], в которой он достаточно подробно описал схему быстрого развертывания Кибер Бэкап. Описания настроек UrBackup также можно встретить в интернете, однако почти все статьи довольно старые (больше 10 лет), кроме того, что предлагает нам ALT Linux Wiki [9], официальная документация ОС Альт Сервер [1] и статья, представленная на портале Яндекс Дзен. В последней статье [6] подробно приведена возможная настройка сервиса на операционной системе Ubuntu. Если говорить о сравнении двух исследуемых продуктов для резервного копирования, то информации в интернете нет, и именно с этим связана новизна и актуальность данной работы.

Таблица 1 – Основные характеристики

Категория	UrBackup	КиберБэкап
Архитектура	<i>Клиент-серверная:</i> сервер создает резервные копии данных с клиентов. Клиенты работают на Windows, Linux, FreeBSD.	<i>Клиент-серверная:</i> сервер управляет агентами, предоставляет веб-интерфейс и обрабатывает планы резервного копирования.
Платформы	<i>Сервер:</i> работает на Windows, GNU/Linux, FreeBSD. <i>Клиент:</i>	<i>Сервер:</i> работает на Windows и Linux. <i>Клиент:</i>

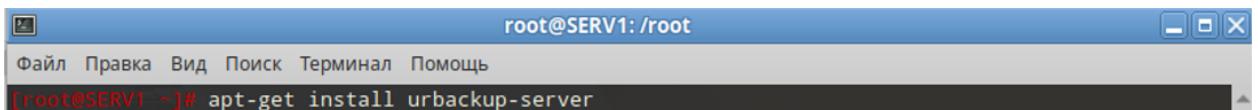
	поддерживает Windows, Linux, FreeBSD. Только клиент Windows поддерживает резервное копирование образов дисков.	поддерживает Windows, Linux, виртуальные платформы VMWare, Hyper-V и OpenStack.
Управление	Веб-интерфейс, cli	Веб-интерфейс, cli
Типы резервного копирования	<i>Файлы:</i> полное, инкрементное <i>Образы:</i> полные и инкрементные копии разделов дисков (в Windows)	<i>Файлы:</i> полное, инкрементное, дифференциальное <i>Образы:</i> возможность создания резервных копий дисков и виртуальных машин.
Настройка резервных копий	Возможность настройки расписания, дедупликация, ограничения на количество хранимых резервных копий. Поддержка современных файловых систем	Возможность настройки расписания, дедупликация, ограничения на количество хранимых резервных копий. Поддержка современных файловых систем
Безопасность	<i>Аутентификация:</i> используются открытые и закрытые ключи (ECDSA), поддерживается проверка подлинности сервера. <i>Шифрование передачи:</i> в интернет-режиме используются AES-GCM и HMAC-SHA512.	<i>Аутентификация:</i> Используются сертифицированные алгоритмы аутентификации и шифрования (AES, SSL/TLS). <i>Шифрование передачи:</i> Поддержка шифрования как передаваемых данных, так и хранилища резервных копий.

Инструменты имеют схожие характеристики, но в отличие от UrBackup Кибербэkap обладает более обширным функционалом и поддержкой резервного копирования виртуальных машин

UrBackup – это простая в настройке система резервного копирования, работающая по архитектуре клиент-сервер. Она поддерживает кроссплатформенность и предоставляет широкие возможности для резервного копирования данных.

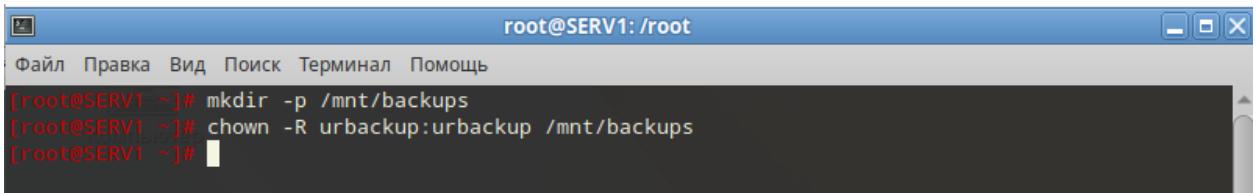
Для работы развернем систему во внутренней сети Клиент-Сервер.

1. Установка сервера:



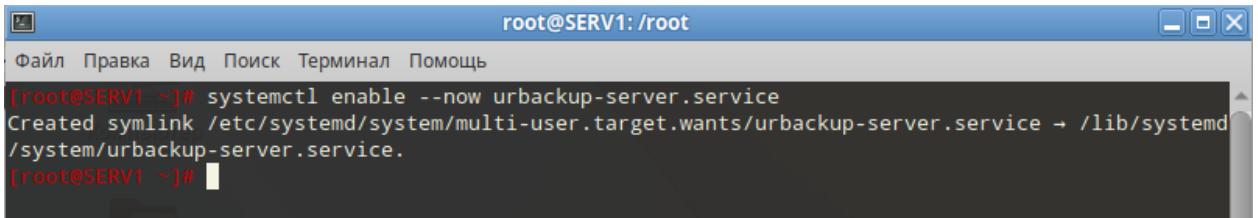
```
root@SERV1: /root
Файл Правка Вид Поиск Терминал Помощь
[root@SERV1 ~]# apt-get install urbackup-server
```

2. Создание каталога для резервных копий и настройка прав на него:



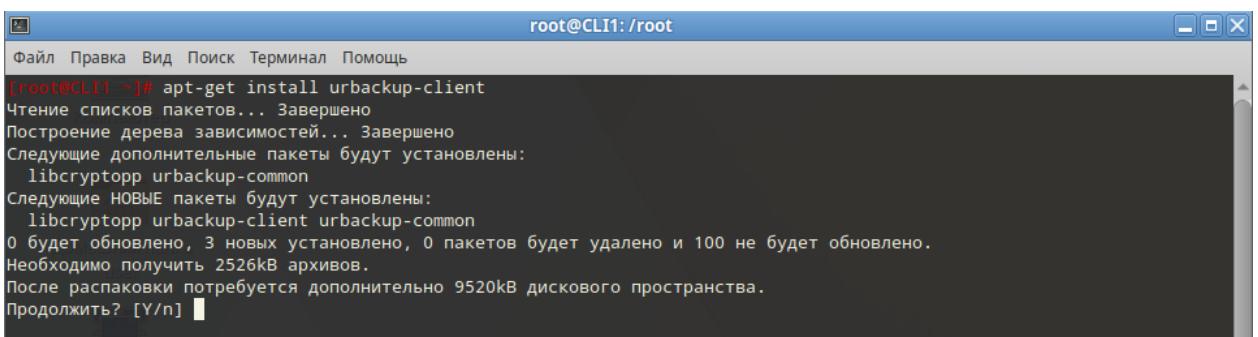
```
root@SERV1: /root
Файл Правка Вид Поиск Терминал Помощь
[root@SERV1 ~]# mkdir -p /mnt/backups
[root@SERV1 ~]# chown -R urbackup:urbackup /mnt/backups
[root@SERV1 ~]#
```

3. Настройка автозагрузки сервиса:



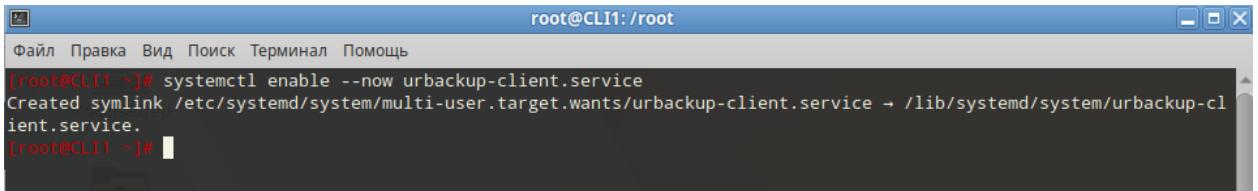
```
root@SERV1: /root
Файл Правка Вид Поиск Терминал Помощь
[root@SERV1 ~]# systemctl enable --now urbackup-server.service
Created symlink /etc/systemd/system/multi-user.target.wants/urbackup-server.service → /lib/systemd
/system/urbackup-server.service.
[root@SERV1 ~]#
```

4. Установка клиента:



```
root@CLI1: /root
Файл Правка Вид Поиск Терминал Помощь
[root@CLI1 ~]# apt-get install urbackup-client
Чтение списков пакетов... Завершено
Построение дерева зависимостей... Завершено
Следующие дополнительные пакеты будут установлены:
 libcryptopp urbackup-common
Следующие НОВЫЕ пакеты будут установлены:
 libcryptopp urbackup-client urbackup-common
0 будет обновлено, 3 новых установлено, 0 пакетов будет удалено и 100 не будет обновлено.
Необходимо получить 2526kB архивов.
После распаковки потребуется дополнительно 9520kB дискового пространства.
Продолжить? [Y/n] ■
```

5. Настройка автозапуска сервиса на клиенте:



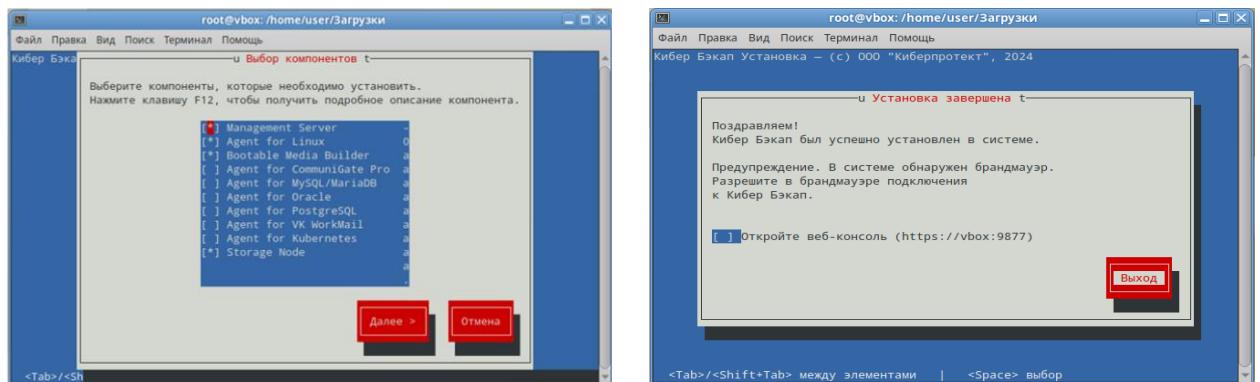
```
root@CLI1: /root
Файл Правка Вид Поиск Терминал Помощь
[root@CLI1 ~]# systemctl enable --now urbackup-client.service
Created symlink /etc/systemd/system/multi-user.target.wants/urbackup-client.service → /lib/systemd/system/urbackup-cl
ient.service.
[root@CLI1 ~]#
```

«Кибер Бэкап» (ранее Acronis Защита Данных) – система резервного копирования, восстановления и защиты данных для ИТ-систем любой сложности с централизованным управлением и оптимизацией хранения. Решение работает с любыми системами в организациях любого размера – от малого предприятия до крупной корпорации.

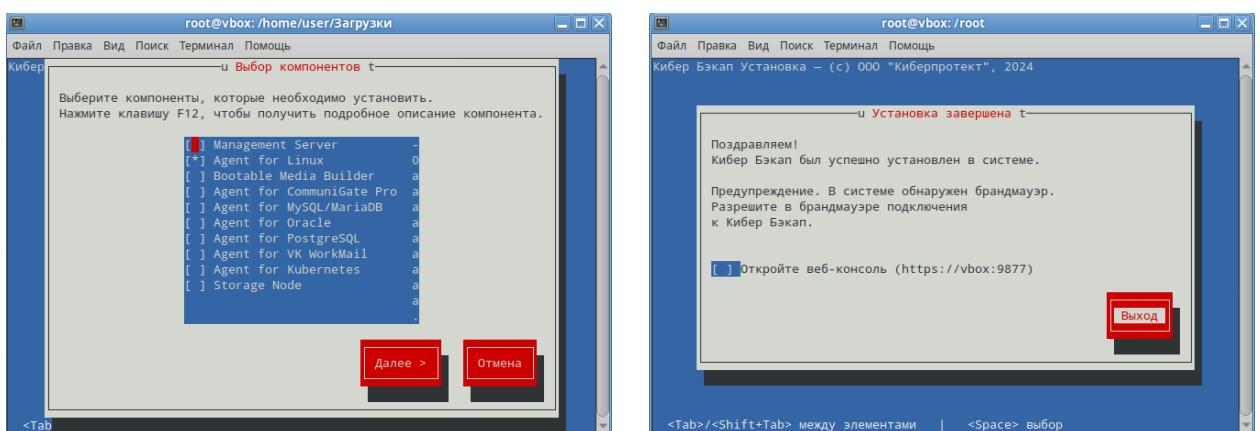
Система поддерживает широкий спектр платформ, серверов и рабочих станций, операционных систем, систем виртуализации и приложений. Кибер Бэкан входит в реестр российского ПО Минцифры России.

Проведем настройку сервиса. Для этого необходимо произвести установку сервера и агента.

### 1. Установка сервера:

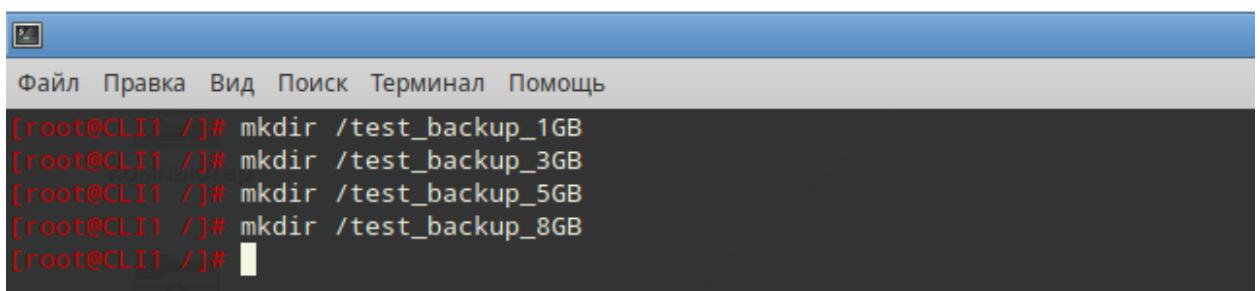


### 2. Установка агента:



## Проведение эксперимента

Для тестирования мы будем применять следующий набор директорий:



```
[root@CLI1 /]# mkdir /test_backup_1GB
[root@CLI1 /]# mkdir /test_backup_3GB
[root@CLI1 /]# mkdir /test_backup_5GB
[root@CLI1 /]# mkdir /test_backup_8GB
[root@CLI1 /]#
```

Директории заполнены файлами 1, 3, 5 и 8 Гб соответственно:

```

[1] # dd if=/dev/urandom of=/test_backup_1GB/file_1GB bs=1GB count=1
1+0 записей получено
1+0 записей отправлено
1000000000 байт (1,0 GB, 954 MiB) скопирован, 32,6153 s, 30,7 MB/s
[1] #

[2] # dd if=/dev/urandom of=/test_backup_3GB/file_3GB bs=1GB count=3
3+0 записей получено
3+0 записей отправлено
3000000000 байт (3,0 GB, 2,8 GiB) скопирован, 129,965 s, 23,1 MB/s
[2] #

[3] # dd if=/dev/urandom of=/test_backup_5GB/file_5GB bs=1GB count=5
5+0 записей получено
5+0 записей отправлено
5000000000 байт (5,0 GB, 4,7 GiB) скопирован, 209,783 s, 23,8 MB/s
[3] #

[4] # dd if=/dev/urandom of=/test_backup_8GB/file_8GB bs=1GB count=8
8+0 записей получено
8+0 записей отправлено
8000000000 байт (8,0 GB, 7,5 GiB) скопирован, 389,348 s, 20,5 MB/s
[4] #

```

Создадим резервные копии этих файлов с помощью системы резервного копирования

Сначала проведем эксперимент с UrBackup.

Каталог размером 1 Гб:

The screenshot shows the UrBackup configuration interface with the 'Настройки' (Settings) tab selected. Under the 'Файловые бэкапы' (File Backups) tab, various backup parameters are set:

- Интервал создания инкрементальных файловых блоков: 5 часов
- Интервал создания полных бэкапов файлов: 30 дней
- Максимальное количество инкрементальных бэкапов файлов: 100
- Минимальное количество инкрементальных бэкапов файлов: 40
- Максимальное количество полных бэкапов файлов: 10
- Минимальное количество полных бэкапов файлов: 2
- Исключить из бэкапа (по маске): (empty)
- Включить в бэкап (по маске): (empty)
- Каталоги по умолчанию для бэкапа: /test\_backup\_1GB;

At the bottom right, there is a 'Сохранить' (Save) button.

Запустим полный файловый бэкап:

The screenshot shows the 'В работе' (In Progress) interface with a single job listed:

Имя компьютера	Действие	Подробности	Прогресс	Расчетное время выполнения	Скорость	Файлов в очереди
CLI1	Полный файловый бэкап	-	38% <div style="width: 38%;"></div> 357.63 MB / 953.67 MB	1 Минута	-	0 <span style="background-color: red; color: white; padding: 2px;">Стоп</span> <span style="border: 1px solid #ccc; padding: 2px;">Показать лог</span>

Время создания резервной копии:

16.01.25 14:56 INFO Time taken for backing up client CLI1: 1m 20s

Таким образом, меняя в настройках каталог для бэкапа, измерим время для остальных директорий.

Каталог размером 3 Гб:

16.01.25 15:03 INFO Time taken for backing up client CLI1: 2m 10s

Каталог размером 5 Гб:

16.01.25 15:14 INFO Time taken for backing up client CLI1: 3m

Каталог размером 8 Гб:

16.01.25 15:34 INFO Time taken for backing up client CLI1: 3m 30s

Перейдем к восстановлению данных. Для этого на клиенте необходимо открыть файл `/etc/sysconfig/urbackupclient` и отредактировать значение параметра “RESTORE”. По умолчанию стоит значение “disabled”, при котором восстановление с веб-интерфейса невозможно. Поставим значение “server-confirms” для восстановления данных с веб-интерфейса сервера:

```
# Valid settings:
#
# "client-confirms": If you have the GUI component the currently active user
#                     will need to confirm restores from the web interface.
#                     If you have no GUI component this will cause restores
#                     from the server web interface to not work
# "server-confirms": The server will ask the user starting the restore on
#                     the web interface for confirmation
# "disabled":        Restores via web interface are disabled.
#                     Restores via urbackupclientctl still work
#
RESTORE=server-confirms
```

Перейдем в веб-интерфейсе сервера во вкладку «Бэкапы», выберем клиента, откроем нужный бэкап и запустим процесс восстановления. Так как в логах не фиксируется время восстановления, будем замерять его вручную.

Восстановление каталога размером 1 Гб:

The screenshot shows the UrBackup web interface. At the top, a header bar displays 'Клиенты >CLI1 > 16.01.25 14:54'. Below this is a table with a single row for a backup named 'test\_backup\_1GB'. The table columns are 'Файл', 'Размер', 'Создано', 'Последнее изменение', and 'Последний доступ'. The 'Восстановление' button in this row is highlighted. At the bottom of this section are two buttons: 'Скачать папки в ZIP архиве' and 'Восстановить папку на клиенте'.

Below this is a blue header bar with the text 'В работе'. Underneath is a table showing the restore progress for the backup. The columns are 'Имя компьютера', 'Действие', 'Подробности', 'Прогресс', 'Расчетное время выполнения', 'Скорость', and 'Файлов в очереди'. The table shows one row for 'CLI1' with the status 'Восстановление', 'Путь: 12% 117.86 MB / 953.67 MB', and a progress bar indicating 12% completion.

Время восстановления – 18 секунд.

Таким образом восстановим и другие каталоги, замеряя при этом время.

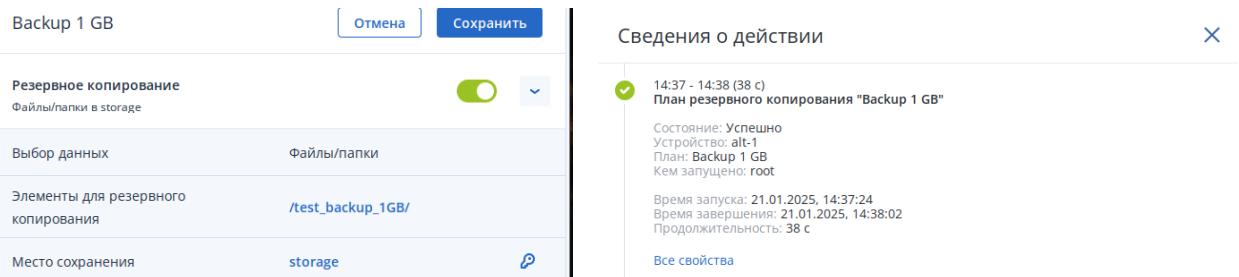
Восстановление каталога размером 3 Гб: 99 секунд.

Восстановление каталога размером 5 Гб: 130 секунд.

Восстановление каталога размером 8 Гб: 220 секунд

Проведем эксперимент с Кибер Бэкап.

Каталог размером 1 Гб



Время резервного копирования – 38 секунд.

Каталог размером 3 Гб – 67 секунд.

Каталог размером 5 Гб – 94 секунд.

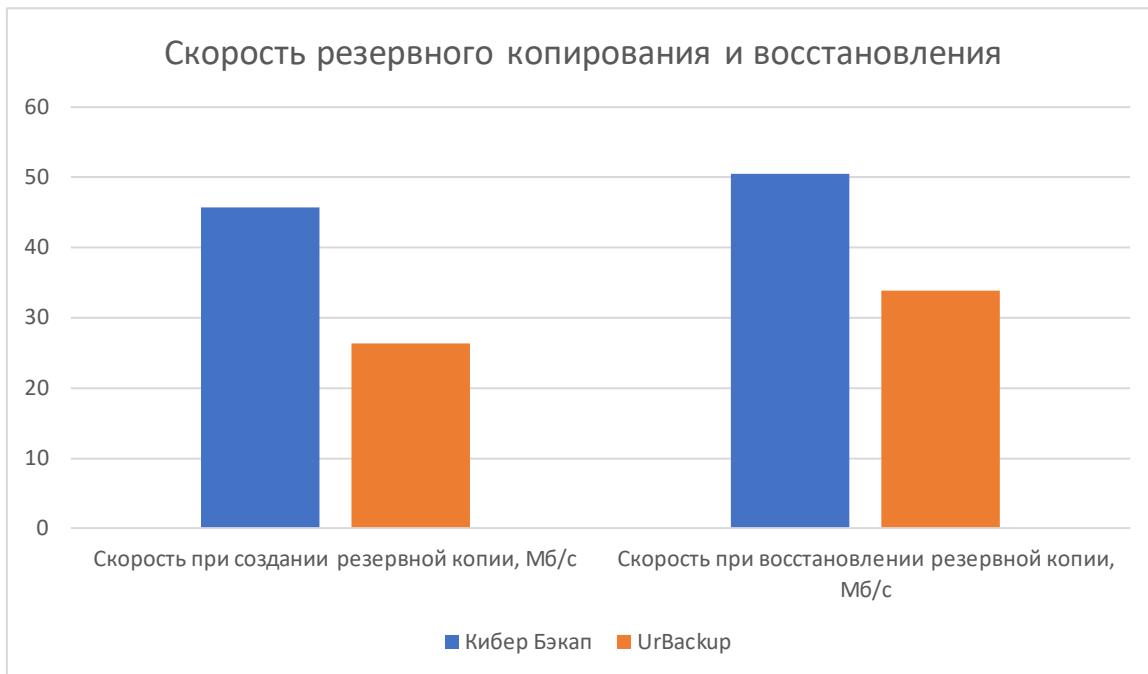
Каталог размером 8 Гб – 148 секунд.

Проведем восстановление резервных копий и представим результаты в таблице 2.

Таблица 2 – Результаты создания и восстановления резервных копий

	Кибер Бэкап		UrBackup	
Размер каталога, Гб	Время создания резервной копии, с	Время восстановления резервной копии, с	Время создания резервной копии, с	Время восстановления резервной копии, с
1	38	25	80	18
3	67	48	130	99
5	94	87	180	130
8	148	154	210	220

Вычислим среднюю скорость передачи данных при создании резервной копии и ее восстановлении и покажем на диаграмме:



## Заключение

Проведённый сравнительный анализ двух решений для резервного копирования и восстановления данных в ОС Альт – UrBackup и Кибер Бэкап – позволил выявить их сильные и слабые стороны. Кибер Бэкап показал явно лучшие результаты, однако стоит учитывать тот факт, что этот продукт является платным в отличие от UrBackup.

## **Список использованных источников**

1. Альт Сервер 10.4. Документация. Руководство пользователя. Редакция ноябрь, 2024. Глава 57 Система резервного копирования UrBackup. [Электронный ресурс]. Режим доступа: <https://docs.altlinux.org/ru-RU/alt-server/10.4/html/alt-server/index.html> (дата обращения: 16.01.2025)
2. Запуск Кибер Бэкап на Альт Сервер 10 [Электронный ресурс]. Режим доступа: <https://dondub.com/2023/05/zapusk-kiber-bekap-na-alt-server-10/> (дата обращения: 18.01.2025)
3. Кибер Бэкап: Быстрый старт на Linux. [Электронный ресурс]. Режим доступа: <https://habr.com/ru/companies/cyberprotect/articles/836172/> (дата обращения: 19.01.2025)
4. Кибер Бэкап Версия 17.2. Руководство пользователя. [Электронный ресурс]. Режим доступа: [https://docs.cyberprotect.ru/ru-RU/CyberBackup/17.2/CyberBackup\\_userguide\\_ru-RU.pdf](https://docs.cyberprotect.ru/ru-RU/CyberBackup/17.2/CyberBackup_userguide_ru-RU.pdf) (дата обращения: 17.01.2025)
5. Кибер Бэкап и ОС Linux. [Электронный ресурс]. Режим доступа: <https://habr.com/ru/companies/cyberprotect/articles/828446/> (дата обращения: 18.01.2025)
6. Резервное копирование в организации на Ubuntu 22.04LTS + UrBackup 2.5.27. [Электронный ресурс]. Режим доступа: <https://dzen.ru/a/Y5gnQ456Cyy1qaYg> (дата обращения: 19.01.2025)
7. Уймин, А. Г. Периферийные устройства ЭВМ: Практикум / А. Г. Уймин. – Москва: Ай Пи Ар Медиа, 2023. – 429 с. – ISBN 978-5-4497-2079-5. – EDN KQQFAG (дата обращения: 16.01.2025)
8. Administration Manual for UrBackup Server 2.5.x. Martin Raiber. August 27, 2022. [Электронный ресурс]. Режим доступа: [https://www.urbackup.org/administration\\_manual.html](https://www.urbackup.org/administration_manual.html) (дата обращения: 17.01.2025)
9. UrBackup – ALT Linux Wiki. [Электронный ресурс]. Режим доступа: <https://www.altlinux.org/UrBackup> (дата обращения: 16.01.2025)