

WHITE PAPER

МЕХАНИЗМ САНПШОТОВ В TATLIN.BACKUP.
ПРИМЕНЕНИЕ СНАПШОТОВ В КИБЕРБЭКАП





О WHITE PAPER

Данный документ описывает архитектурные принципы и подходы, а также рекомендации по их применению при построении корпоративных решений на основе продуктов производства компании YADRO.

Документ предназначен для широкой аудитории, но также может включать материалы, требующие специальной профессиональной подготовки, ориентированные на системных архитекторов, администраторов, сервисных инженеров и других IT-специалистов, участвующих в планировании, проектировании и внедрении комплексных решений.

! Представленная информация основана на результатах исследований, а также экспертизе специалистов YADRO. Документ носит не предписывающий, а информационный характер, целью которого является информирование получателей документа о предмете произведенного исследования и о его результатах. При этом конкретные результаты и эффективность конечных решений зависят от множества факторов, которые могут различаться в зависимости от особенностей инфраструктуры и условий эксплуатации. Ни при каких обстоятельствах YADRO не несет ответственность за последствия применения получателем документа рекомендаций, инструкций, подходов и решений, указанных в документе.

Запрещается копировать, воспроизводить, изменять, публиковать, передавать, распространять, продавать информацию (часть информации), содержащуюся в документе, или создавать производные работы на основе содержания документа без предварительного письменного разрешения YADRO.

Любая информация или утверждения относительно возможностей, емкости, производительности или других характеристик продукции, указанной в документе, предоставляются исключительно на условиях «как есть» и приведена исключительно в целях описания произведенного исследования. YADRO оставляет за собой право вносить изменения/обновлять информация в документе без уведомления.

«YADRO» является зарегистрированным товарным знаком ООО «КНС ГРУПП». Другие названия продуктов и компаний, упомянутые здесь, могут быть товарными знаками или торговыми наименованиями их соответствующих владельцев.

Актуальные версии документации публикуются на информационном ресурсе YADRO по адресу service.yadro.com.

ОГЛАВЛЕНИЕ

1.	ОБ ЭКСПЕРТАХ	4
2.	ВВЕДЕНИЕ	5
3.	СНАПШОТЫ И ИХ ПРЕДНАЗНАЧЕНИЕ.....	6
4.	ПРИНЦИП РАБОТЫ СНАПШОТОВ.....	7
5.	ВИДЫ СНАПШОТОВ И УПРАВЛЕНИЕ РАСПИСАНИЕМ.....	8
6.	ПРАКТИЧЕСКИЕ СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ СНАПШОТОВ	9
6.1.	Восстановление на уровне хранилища.....	9
6.2.	Восстановление через экспорт снапшота.....	12
7.	ЗАКЛЮЧЕНИЕ.....	17

ОБ ЭКСПЕРТАХ

Алексей Головин — специалист с 15-летним опытом работы в сфере ИТ, включая опыт в таких компаниях, как Dell EMC и системных интеграторах. В команде YADRO занимает позицию ведущего специалиста по интеграционным решениям. Алексей поддерживает сложную инфраструктуру корпоративных клиентов.

Занимается настройкой, оптимизацией и обслуживанием хранилищ данных и инфраструктуры резервного копирования. Специализируется на диагностике и устранении неисправностей систем YADRO, DellEMC, Cisco, Brocade, Pivotal и других производителей..

ВВЕДЕНИЕ

В последнее время потребность в снимках для резервного копирования стремительно возросла: угрозы шифровальщиков и риск потери логической целостности данных потребовали пересмотра стратегии. Команда TATLIN.BACKUP разработала и внедрила собственный механизм создания мгновенных снимков (снимотов), который будет подробно рассмотрен в следующих разделах.

ВЕРСИИ ИСПОЛЪЗУЕМОГО ПО

TATLIN.BACKUP.M	1.3
Кибер Бэкап	18

СНАПШОТЫ И ИХ ПРЕДНАЗНАЧЕНИЕ

Снапшот – общепринятый в отрасли термин, обозначающий фиксацию состояния устройства хранения данных или части данных, хранящихся на нем, в заданный момент времени с возможностью последующего восстановления. Снапшот фиксирует состояние данных на определенный момент времени.

Создание снапшота происходит мгновенно. После этого он становится доступным для использования другими приложениями, такими как средства защиты данных, аналитики и отчетности. При этом исходные данные остаются доступными для приложений без прерывания работы, а снапшот может использоваться для выполнения других операций с данными.

Снапшоты – надежный механизм защиты данных. Тенденция к использованию снапшотов обусловлена их существенными преимуществами при решении многих задач компаний.

Снапшоты обеспечивают:

- более высокую доступность приложений;
- ускоренное восстановление данных;
- упрощенное управление резервным копированием больших объемов данных.

Ключевые преимущества снапшотов:

- Создание снапшотов происходит практически мгновенно и не требует значительных вычислительных или дисковых ресурсов.
- Снапшоты фиксируют состояние выбранной VFS в режиме Read Only и удерживают все данные, на которые они ссылаются. Снапшоты обеспечивают сохранность зафиксированного состояния даже при удалении, изменении или повреждении исходных данных в оригинальной VFS, а также после истечения срока хранения резервных копий.
- Снапшот, созданный после резервного копирования, позволяет восстановиться, даже если злоумышленник зашифрует данные на VFS, которая остается доступной для записи и изменений.
- Снапшоты в TATLIN.BACKUP можно монтировать в отдельные точки монтирования в режиме Read Only, что позволяет сравнивать данные или извлекать отдельные файлы без влияния на исходную VFS.
- TATLIN.BACKUP позволяет создавать снапшоты VFS, настраивать их типы и расписания, а также отслеживать состояние существующих снапшотов.

ПРИНЦИП РАБОТЫ СНАПШОТОВ

Снапшот в TATLIN.BACKUP создается мгновенно без перезаписи данных. В момент создания система фиксирует состояние выбранной VFS и предотвращает удаление и изменение связанных с ней данных, поэтому создание снапшота не требует дополнительного дискового пространства. Новые или измененные данные записываются в новое место в соответствии с политикой Copy-on-Write (COW).

Операция создания снапшота выполняется практически мгновенно и оказывает минимальную нагрузку на систему. Блоки данных защищаются от удаления, пока на них ссылается хотя бы один существующий снапшот. Снапшот сохраняет состояние выбранной VFS в режиме Read Only на заданный момент времени (например, 18:00).



При изменении файловых данных добавляются новые блоки, а указатели на изменённые блоки сохраняются в журналах основной системы. Снапшот при этом хранит ссылки на оригинальные данные в момент создания — никакие данные не перезаписываются и не удаляются.

При изменении файлов (старые блоки 1 и 2) новые данные записываются в отдельные блоки (5 и 6), а активная файловая система переназначает на них ссылки. Оригинальные блоки остаются неизменными, поскольку снапшот сохраняет ссылки на них. Блоки удаляются из хранилища, когда на них не остается ссылок ни в одной из текущих VFS, ни в каких-либо снапшотах.

Такой подход обеспечивает мгновенное создание точек восстановления, минимальную нагрузку на систему и гарантированную сохранность данных до момента, когда они перестанут быть нужными.

ВИДЫ СНАПШОТОВ И УПРАВЛЕНИЕ РАСПИСАНИЕМ

В TATLIN.BACKUP реализованы три уровня защиты снимков.

Для всех уровней действует общее правило: снимок автоматически удаляется по истечении заданного срока хранения. Ручное изменение или удаление снимка определяется уровнем защиты и ролевой моделью доступа.

- Basic — изменение параметров и удаление снимка доступны пользователям с ролью admin.
- Secure — модификация атрибутов снимка доступна только пользователям с ролью security. Пользователь с ролью admin может удалить снимок только после понижения уровня его защиты до Basic.
- Locked — ручное изменение или удаление снимка недоступно пользователям системы. Управление таким снимком возможно только при участии сервисного инженера YADRO.

Разграничение ролей позволяет защитить критические снимки даже при компрометации учетных данных администратора.

Создание расписания снимков

Расписание снимков организует автоматическое создание и «устаревание» точек восстановления, обеспечивая скользящее окно безопасности.

1. В веб-интерфейсе TATLIN.BACKUP перейдите в **Хранилище – Виртуальные файловые системы**.
2. Выберите необходимую VFS.
3. Перейдите на вкладку **Защита данных**.
4. В блоке **Расписания** нажмите **Создать**.
5. Введите имя расписания и выберите тип защиты (Basic, Secure или Locked).
6. Настройте периодичность по индивидуальному расписанию.
7. Сохраните расписание – снимки будут создаваться автоматически в заданные интервалы.

Автоматическое устаревание

TATLIN.BACKUP поддерживает механизм «устаревания» снимков: когда срок их хранения выходит за пределы заданного окна (например, 7 дней), самые старые точки автоматически становятся доступными для удаления (при снятии блокировки), а новое окно продолжает двигаться вперед. Это обеспечивает:

- постоянное скользящее окно защиты данных, в рамках которого сохраняются только актуальные снимки за последние N дней, без накопления устаревших данных в хранилище;
- предсказуемое и контролируемое использование дискового пространства за счет автоматического удаления снимков по истечении срока хранения в соответствии с заданной политикой;
- гибкость и безопасность управления, поскольку администраторы и службы безопасности могут реализовывать собственные политики хранения, доступа и защиты снимков;
- применение снимков в задачах кибербезопасности, включая защиту данных от шифровальщиков, расследование инцидентов и восстановление к доверенному состоянию.

Современный ландшафт киберугроз стремительно усложняется: растет число атак вымогателей, злоумышленники применяют все более изощренные методы и остаются в сети месяцами, а организации не успевают своевременно выявлять и реагировать на инциденты. В таких условиях снимки становятся одним из ключевых инструментов защиты. Они позволяют мгновенно зафиксировать состояние данных до атаки и быстро восстановить их до «чистой» версии при обнаружении заражения или ошибок. Кроме того, снимки можно монтировать на отдельные серверы или в изолированные тестовые среды, где специализированное ПО проверяет данные и резервные копии на наличие вредоносного ПО, уязвимостей и нарушения целостности. Это повышает отказоустойчивость, сокращает время простоя приложений и минимизирует финансовые и репутационные потери.

Основные показатели текущего ландшафта угроз:

- 82 % случаев утечек мотивированы финансово (Verizon Data Breach Investigations Report 2023).
- 46 % обнаруженного вредоносного ПО – программы-вымогатели (Verizon DBIR 2023).
- CAGR числа вариантов вымогателей 2010–2022 гг. составляет 78 % (SecureWorks State of Cybercrime 2023).
- В среднем организации обнаруживают факт атаки через 120 дней после компрометации (Ponemon Institute, Global Threat Report 2024).
- Медианное время «проживания» угрозы в сети – 105 дней (FireEye Cyber Threat Report 2024).
- Только 28 % организаций довольны своей способностью быстро обнаруживать и расследовать атаки (Gartner, 2024).
- 65 % компаний признают, что восстановление из резервных копий – ключевой ответ на атаки-вымогатели (SecureWorks Ransomware Defense Survey 2023).
- 70 % директоров по кибербезопасности участвуют в планировании восстановления данных как части процесса реагирования на инциденты (Enterprise Strategy Group, 2024).

ПРАКТИЧЕСКИЕ СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ СНАПШОТОВ

В этом разделе приведены результаты испытаний механизма создания и восстановления снимков в среде резервного копирования TATLIN.BACKUP 1.3.x, Кибер Бэкап 18.x.

Цель тестирования – подтвердить корректность, стабильность и предсказуемость работы функций снимков и восстановления данных.

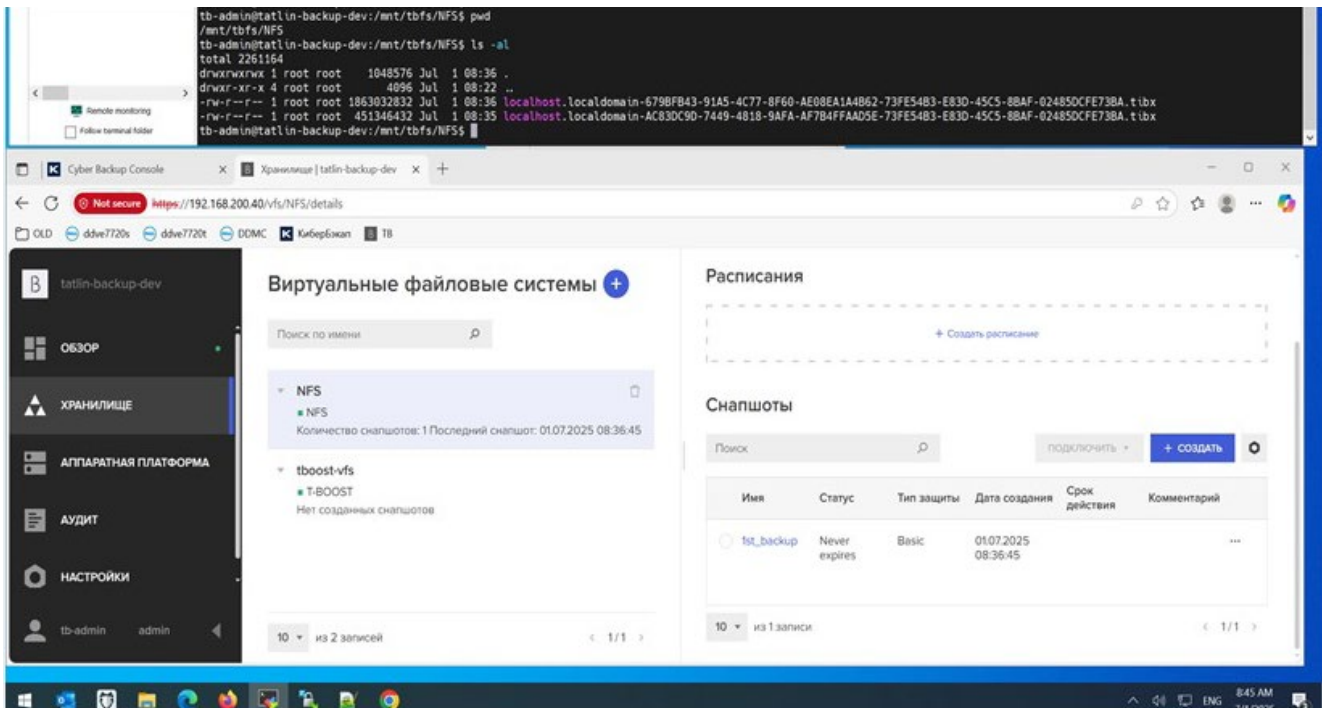
Проверяется механизм создания снимков в TATLIN.BACKUP, целостность и возможность восстановления данных после удаления или повреждения оригинальных файлов:

- Создание резервной копии данных.
- Успешное завершение каждого задания резервного копирования и проверка целостности данных.
- Создание снимка соответствующего хранилища.
- Имитирование инцидента.
- (На подключенном хранилище) сознательное удаление или искажение файлов, попавших в архивы резервных копий.
- Восстановление из ранее созданного снимка.
- Проверка целостности данных.

В ходе тестирования оба сценария восстановления – восстановление данных на уровне хранилища и восстановление через экспорт снимка – были успешно выполнены с использованием соответствующих снимков без потери целостности данных и дополнительных задержек. Подтверждено, что механизм снимков TATLIN.BACKUP можно использовать не только для полного восстановления данных, но и для оперативного доступа к ним непосредственно из снимка. Созданные снимки могут быть смонтированы на хосты по поддерживаемым протоколам доступа (NFS, SMB, T-BOOST), предоставляя консистентное и неизменяемое представление данных на момент их создания и не оказывая влияния на текущее рабочее хранилище.

Восстановление на уровне хранилища

1. Проверка состояния хранилища и наличия файлов резервных копий:



2. Прохождение валидации резервных копий:

CYBERPROTECT							Activities
DASHBOARD							?
Overview							
Alerts							
Activities							
DEVICES							
PLANS							
SOFTWARE MANAGEMENT							
BACKUP STORAGE							
REPORTS							
AUDIT							
SETTINGS							
Q	Device name	search	Any status	Any type	Show all	From:	To:
✓ Refresh automatically							
Status	Description	Device	Start time	Finish time	Duration	S	⚙
✓ Succeeded	Validating backup		01.07.2025 08:49:38	01.07.2025 08:50:06	28 sec	root	
✓ Succeeded	Validating backup		01.07.2025 08:48:48	01.07.2025 08:49:34	46 sec	root	
✓ Succeeded	Deleting backups	localhost.localdomain	01.07.2025 08:35:52	01.07.2025 08:36:03	11 sec	root	
✓ Succeeded	Backup plan 'Local_Downlo...	localhost.localdomain	01.07.2025 08:35:16	01.07.2025 08:35:51	35 sec	root	
✓ Succeeded	Backup plan 'New protectio...	localhost.localdomain	01.07.2025 08:35:13	01.07.2025 08:35:28	15 sec	root	
✓ Succeeded	Applying the protection pla...	localhost.localdomain	01.07.2025 08:34:49	01.07.2025 08:34:49	0 sec	root	
✓ Succeeded	Creating the protection pla...		01.07.2025 08:34:49	01.07.2025 08:34:49	0 sec	root	
✓ Succeeded	Backup plan 'New protectio...	localhost.localdomain	01.07.2025 08:30:09	01.07.2025 08:30:36	27 sec	root	
✓ Succeeded	Logging in account 'root'		01.07.2025 08:29:41	01.07.2025 08:29:41	0 sec		
✓ Succeeded	Synchronizing storage node...		01.07.2025 08:22:49	01.07.2025 08:22:49	0 sec		
✓ Succeeded	Backup plan 'New protectio...	localhost.localdomain	30.06.2025 23:34:46	30.06.2025 23:35:46	60 sec	root	

3. Эмуляция работы шифровальщика или недобросовестного персонала: перезапись файлов и проверка контрольных сумм:

```

root@tatlin-backup-dev:/mnt/tbfs/NFS# ls -al
total 2261164
drwxrwxrwx 1 root root 1048576 Jul 1 08:36 .
drwxr-xr-x 4 root root 1048576 Jul 1 09:17 ..
-rw-r--r-- 1 root root 1863032832 Jul 1 08:36 localhost.localdomain-679BF843-91A5-4C77-8F60-AE08EA1A4B62-73FE54B3-E83D-45C5-8BAF-02485DCFE73BA.tibx
root@tatlin-backup-dev:/mnt/tbfs/NFS# md5sum localhost.localdomain-679BF843-91A5-4C77-8F60-AE08EA1A4B62-73FE54B3-E83D-45C5-8BAF-02485DCFE73BA.tibx
17fdcf06a842b672fad0029505b1c6 localhost.localdomain-679BF843-91A5-4C77-8F60-AE08EA1A4B62-73FE54B3-E83D-45C5-8BAF-02485DCFE73BA.tibx
root@tatlin-backup-dev:/mnt/tbfs/NFS# md5sum localhost.localdomain-AC83DCD9-7449-4818-9AFA-AF784FFAAD5E-73FE54B3-E83D-45C5-8BAF-02485DCFE73BA.tibx
e4f6414849bfd7169141050a03b7de7f localhost.localdomain-AC83DCD9-7449-4818-9AFA-AF784FFAAD5E-73FE54B3-E83D-45C5-8BAF-02485DCFE73BA.tibx
root@tatlin-backup-dev:/mnt/tbfs/NFS# dd if=/dev/urandom of=localhost.localdomain-679BF843-91A5-4C77-8F60-AE08EA1A4B62-73FE54B3-E83D-45C5-8BAF-02485DCFE73BA.tibx bs=1
count=512 seek=$((1024*1024)) conv=notrunc
512+0 records in
512+0 records out
512 bytes copied, 0.0135575 s, 37.8 kB/s
root@tatlin-backup-dev:/mnt/tbfs/NFS# dd if=/dev/urandom of=localhost.localdomain-AC83DCD9-7449-4818-9AFA-AF784FFAAD5E-73FE54B3-E83D-45C5-8BAF-02485DCFE73BA.tibx bs=1
count=512 seek=$((1024*1024)) conv=notrunc
512+0 records in
512+0 records out
512 bytes copied, 0.0542855 s, 9.4 kB/s
root@tatlin-backup-dev:/mnt/tbfs/NFS#
root@tatlin-backup-dev:/mnt/tbfs/NFS#
root@tatlin-backup-dev:/mnt/tbfs/NFS#
root@tatlin-backup-dev:/mnt/tbfs/NFS# md5sum localhost.localdomain-AC83DCD9-7449-4818-9AFA-AF784FFAAD5E-73FE54B3-E83D-45C5-8BAF-02485DCFE73BA.tibx
95547db598ac6c11ec2e60f7d338df localhost.localdomain-AC83DCD9-7449-4818-9AFA-AF784FFAAD5E-73FE54B3-E83D-45C5-8BAF-02485DCFE73BA.tibx
root@tatlin-backup-dev:/mnt/tbfs/NFS#

```

4. Повторная валидация резервных копий.
Результат: валидация не пройдена:

The screenshot shows the Cyberprotect 'Activities' page with a list of failed validation tasks. The 'Activity details' pane on the right provides a close-up of one such error.

Status	Description	Device
Error	Validating backup	
Error	Validating backup	
Succeeded	Validating backup	
Succeeded	Validating backup	
Succeeded	Deleting backups	localhost.localdo...
Succeeded	Backup plan 'Local_Downlo...	localhost.localdo...
Succeeded	Backup plan 'New protectio...	localhost.localdo...
Succeeded	Applying the protection pla...	localhost.localdo...
Succeeded	Creating the protection pla...	

Activity details:
 08:56 — 08:56 (26 sec)
 Validating backup
 Status: Error
 Started by: root
 Start time: 01.07.2025 08:56:22
 Finish time: 01.07.2025 08:56:48
 Duration: 26 sec
 Backup is corrupted. Some data in the backup 'nfs://192.168.200.40/mnt/tbfs/NFS%3a/localhost.localdomain-6798FB43-91A5-4C77-8F60-AE08EA1A4862-73FE54B3-E83D-45C5-8BAF-02485DCE73BA.tbfs' might be damaged because of hardware problems.

5. Восстановление VFS из снимка на TATLIN.BACKUP:

The screenshot shows the 'Восстановить NFS' (Restore NFS) dialog box in the TATLIN.BACKUP interface. The dialog asks for confirmation to restore the NFS file system from a snapshot.

Восстановить NFS
 fst_backup

Состояние виртуальной файловой системы вернется к состоянию, в котором она находилась во время создания выбранного снимка.

Чтобы избежать потери данных, перед восстановлением:
 - Создайте снимок с текущей версией виртуальной файловой системы.
 - Убедитесь, что во время восстановления не будет активных операций ввода/вывода.

Вы уверены, что хотите восстановить NFS из fst_backup?

Введите "подтвердить" для подтверждения

6. Проверка целостности данных после восстановления.
Результат: проверка пройдена успешно:

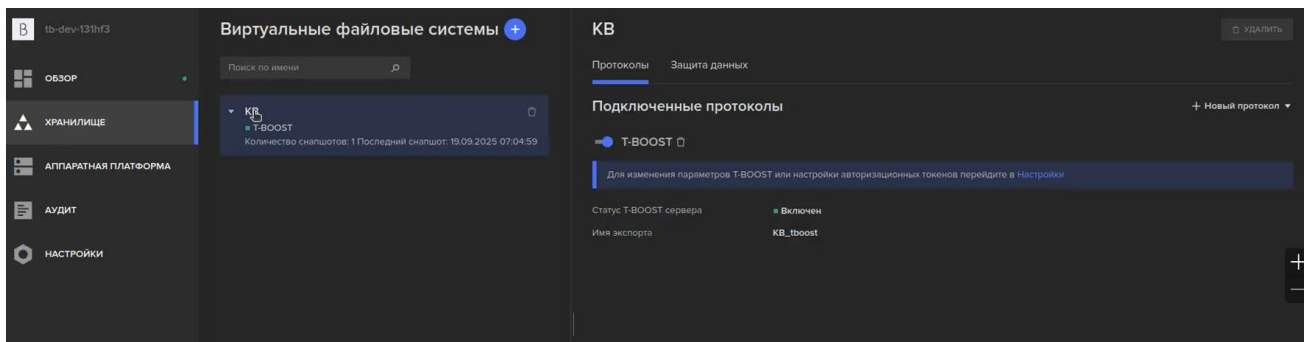
The screenshot shows the Cyberprotect 'Activities' page with a list of successful validation tasks. The 'Activity details' pane on the right provides a close-up of one such success.

Status	Description	Device	Start time	Finish time	Duration	S
Succeeded	Validating backup		01.07.2025 09:12:58	01.07.2025 09:13:26	27 sec	root
Succeeded	Validating backup		01.07.2025 09:12:12	01.07.2025 09:12:41	28 sec	root
Succeeded	Refreshing recovery points		01.07.2025 09:11:27	01.07.2025 09:11:27	0 sec	root
Succeeded	Removing vault from the ag...		01.07.2025 09:03:11	01.07.2025 09:03:11	0 sec	Orga...
Error	Validating backup		01.07.2025 08:56:50	01.07.2025 08:57:15	25 sec	root
Error	Validating backup		01.07.2025 08:56:22	01.07.2025 08:56:48	26 sec	root
Succeeded	Validating backup		01.07.2025 08:49:38	01.07.2025 08:50:06	28 sec	root
Succeeded	Validating backup		01.07.2025 08:48:48	01.07.2025 08:49:34	46 sec	root
Succeeded	Deleting backups	localhost.localdomain	01.07.2025 08:35:52	01.07.2025 08:36:03	11 sec	root

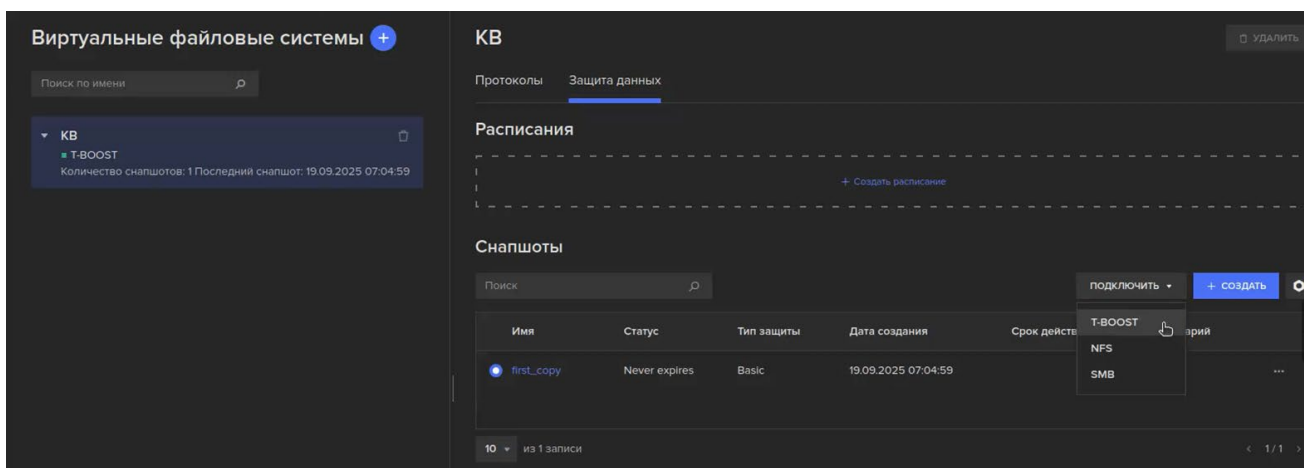
Activity details:
 08:56:23 — 08:56:48
 Running validation plan 'validation Organization 2025-07-01T08:56:21.344995631+03:00'
 Error: Backup is corrupted. Some data in the backup 'nfs://192.168.200.40/mnt/tbfs/NF...

Восстановление через экспорт снимка

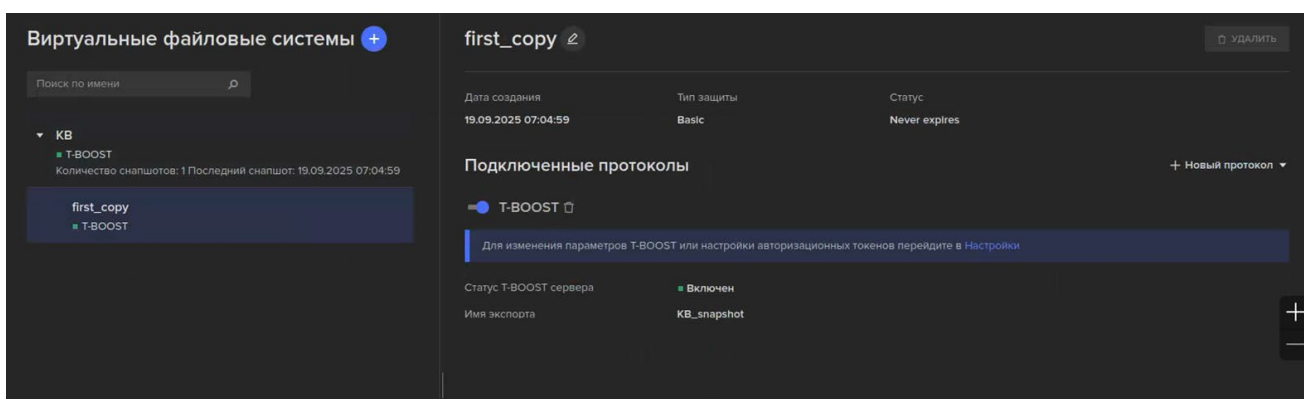
1. Создание снимка на TATLIN.BACKUP:



2. Экспорт снимка по выбранному протоколу (в данном случае T-BOOST):



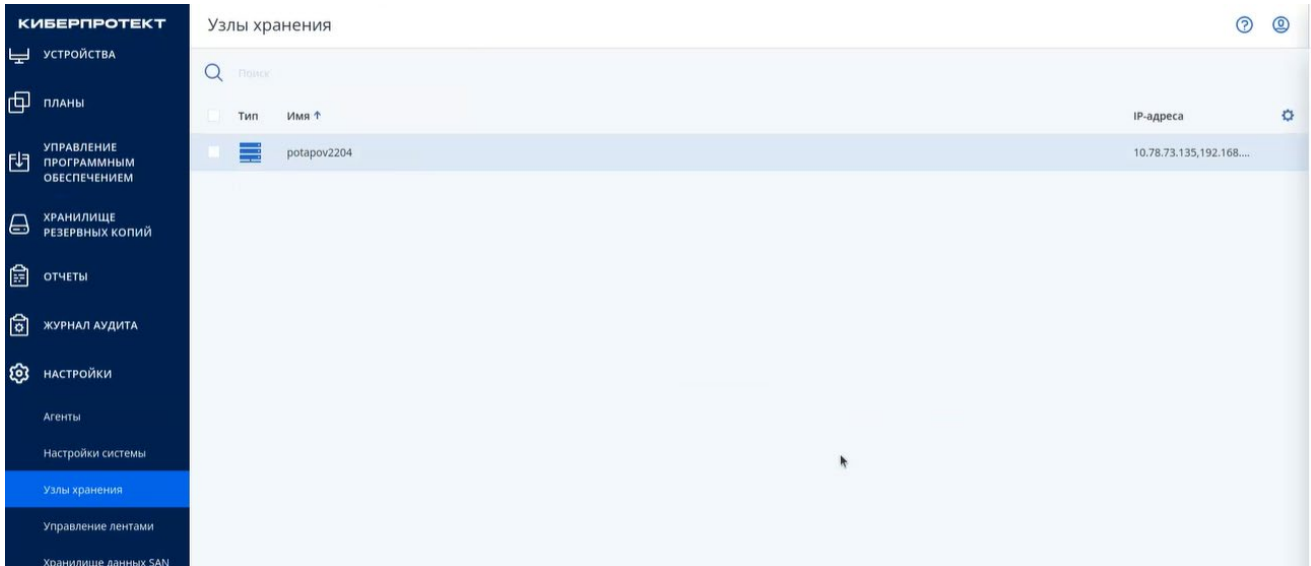
3. Проверка наличия экспорта:



4. Создание временной директории.

Чтобы работать со снимком хранилища, потребовалось обеспечить доступ к метаданным в режиме «чтение + запись»:

- a. Подключиться к узлу хранения по SSH.
- b. Создать временную директорию, в которую будет сохранен снимок метаданных хранилища резервных копий:

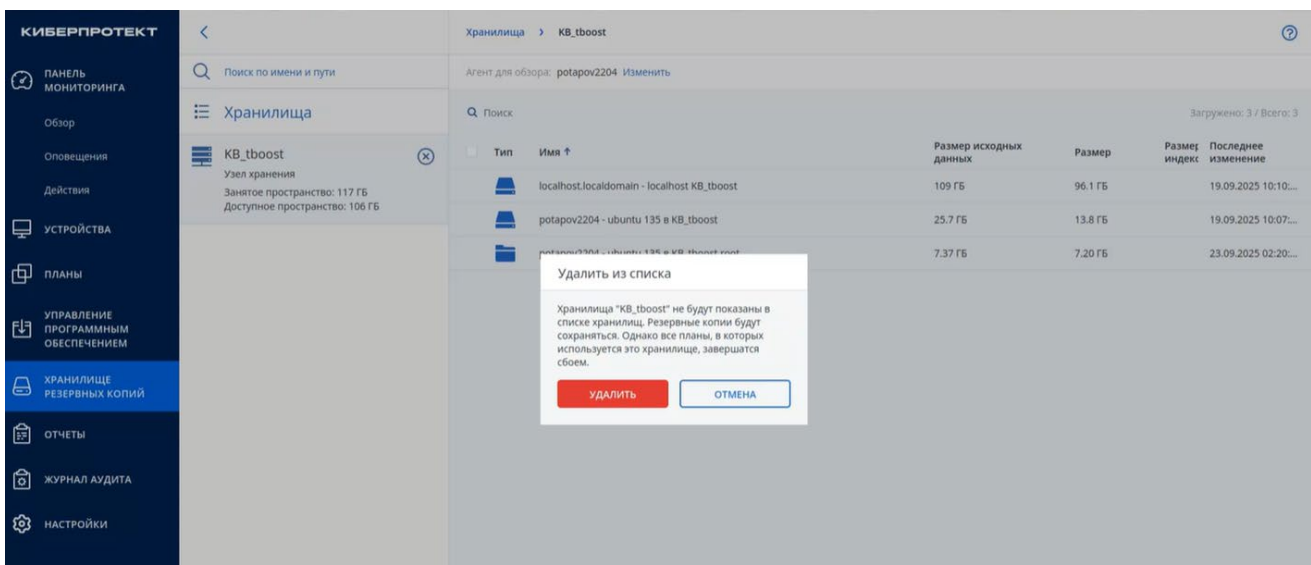


- c. Создать символическую ссылку на директорию с архивами резервных копий:

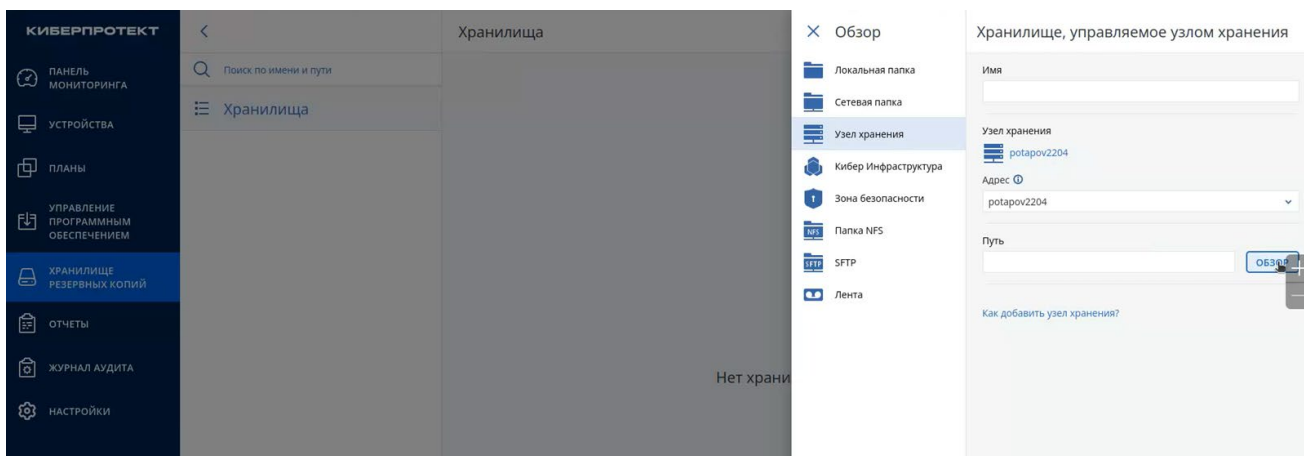
```

root@sntest:~# mkdir /tmp/snapshot
root@sntest:~# tboostctl mount --tcp-addr 192.168.100.108:5555 --export KB_snapshot /tmp/snapshot
Mount ID: 4
root@sntest:~# mkdir /tmp/stor_snapshot
root@sntest:~# cp -r /tmp/snapshot/.meta/ /tmp/stor_snapshot
root@sntest:/tmp/stor_snapshot# cd /tmp/stor_snapshot
root@sntest:/tmp/stor_snapshot# ln -s /tmp/snapshot/computers/ computers
root@sntest:/tmp/stor_snapshot#
    
```

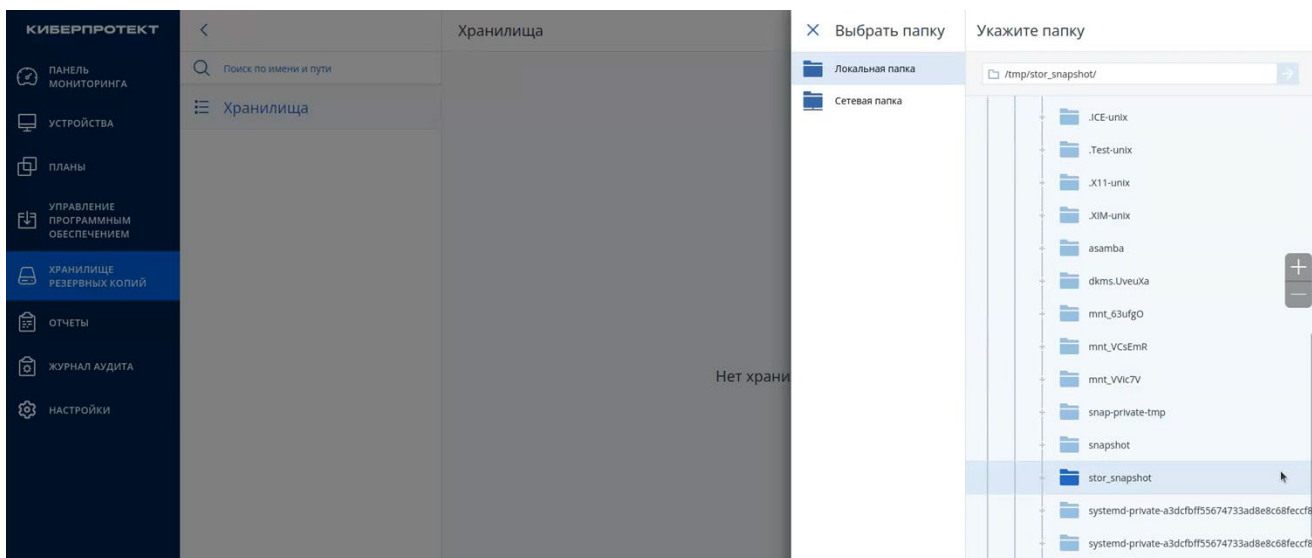
5. Удаление хранилища, выбранного под восстановление из снимка:



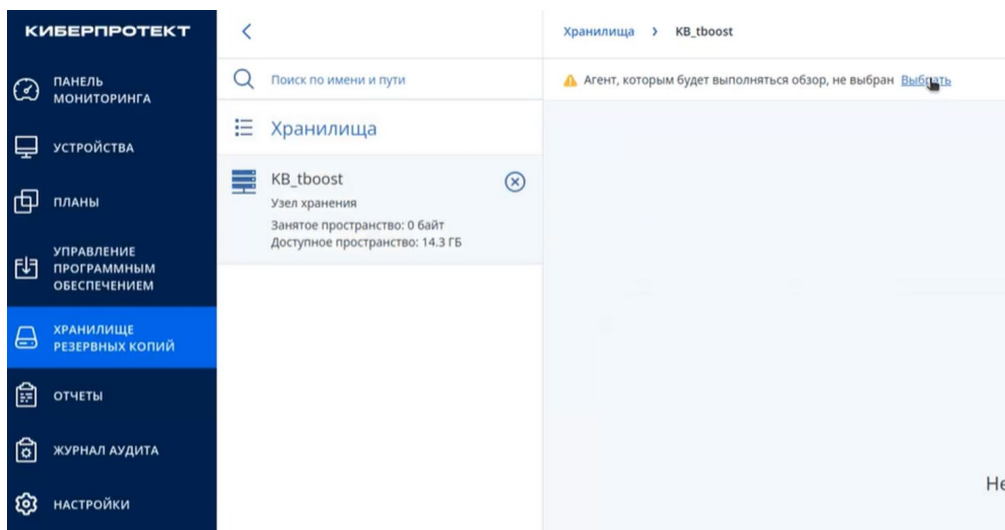
6. Создание хранилища в Кибер Бэкап:



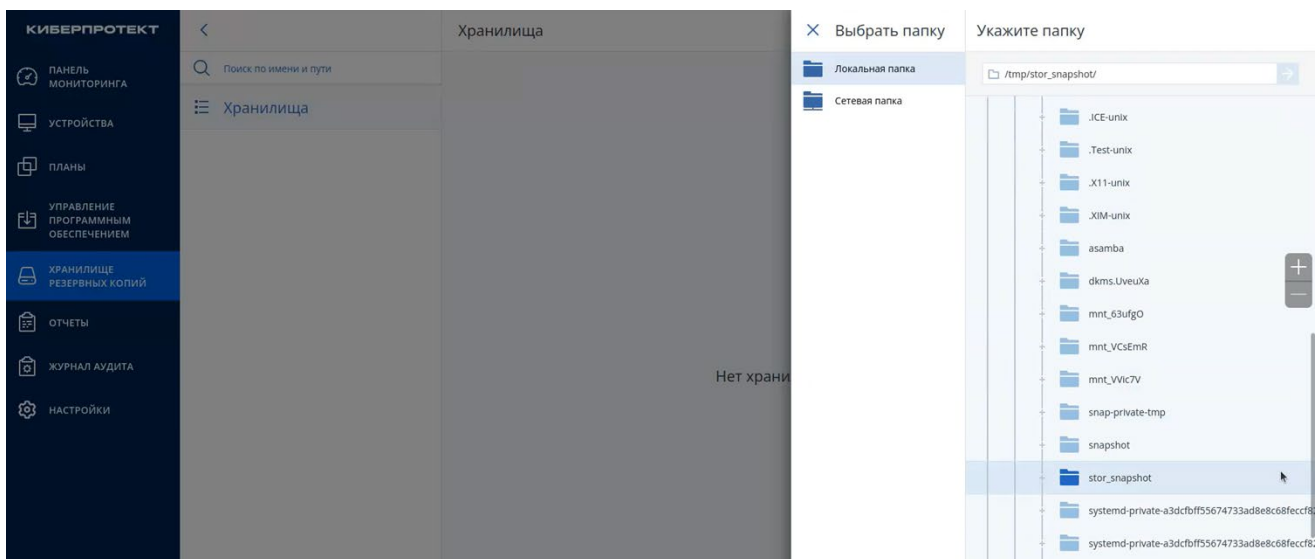
7. Выбор директории с импортированным снимком:



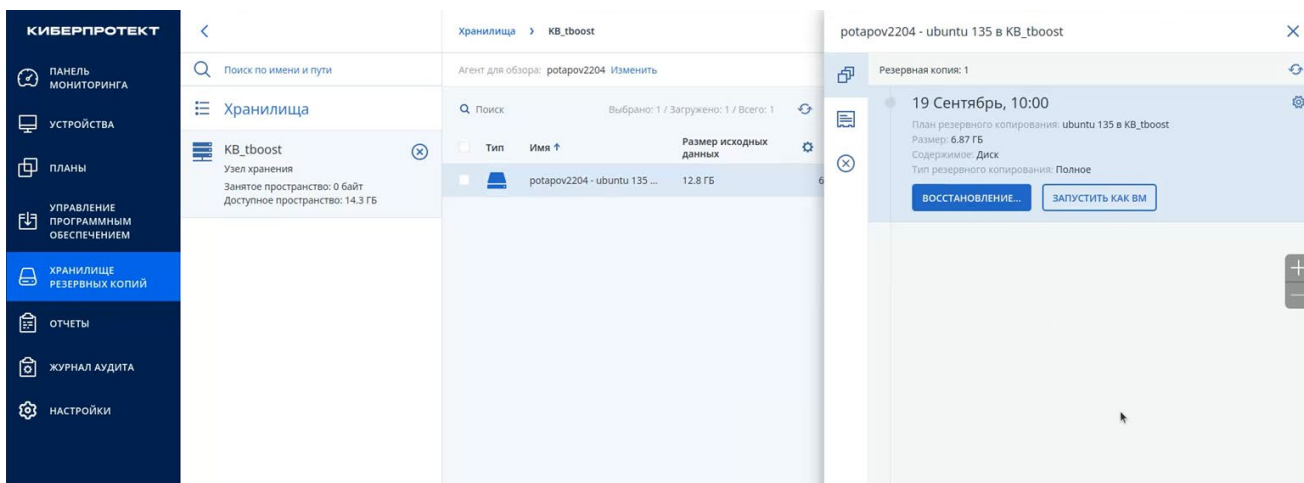
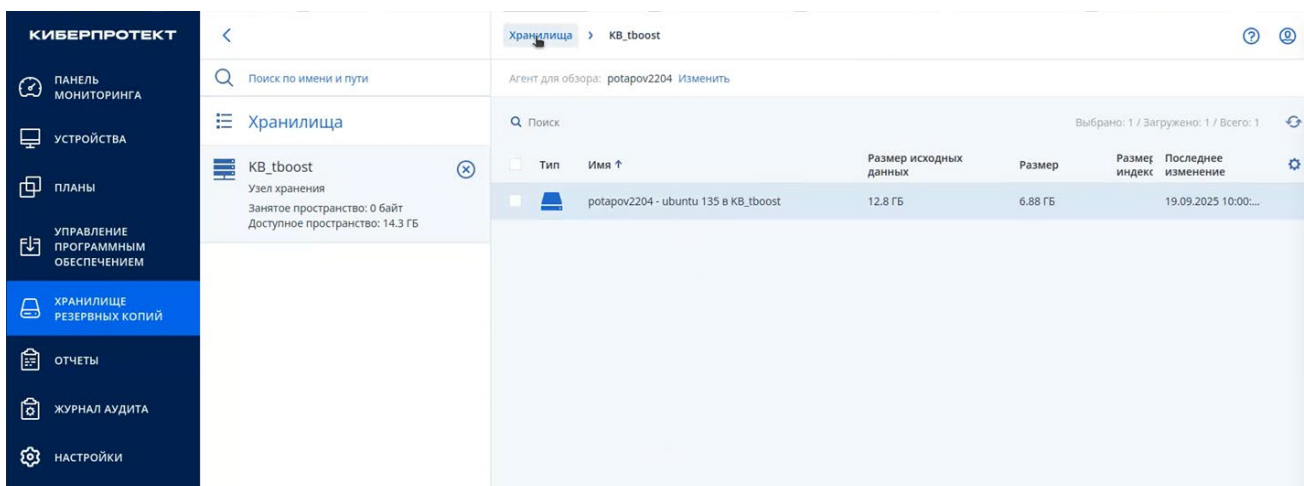
8. Выбор агента:



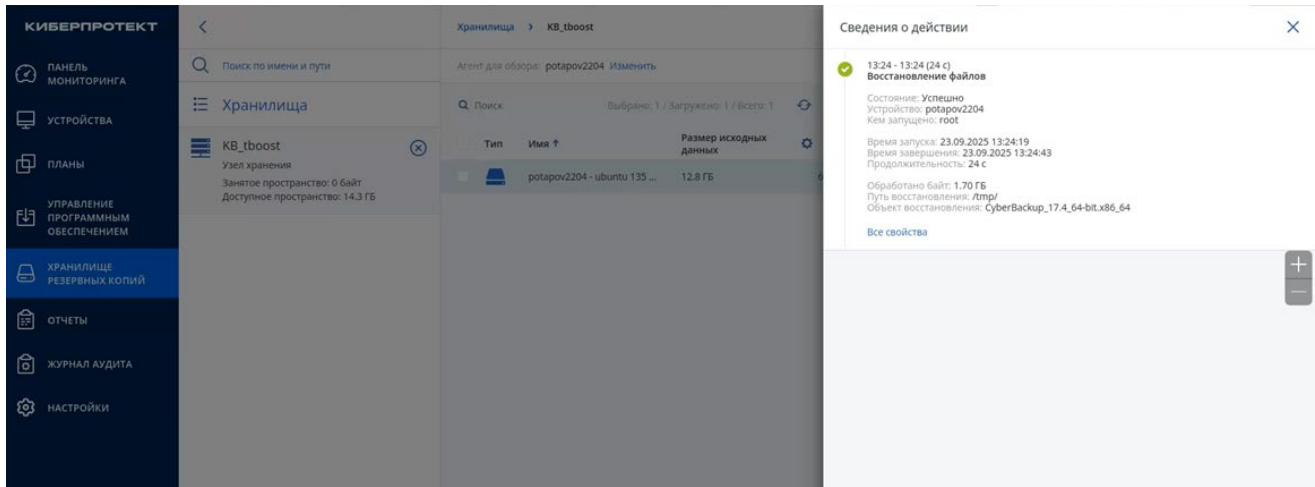
9. Выбор узла хранения, указанного при создании хранилища:



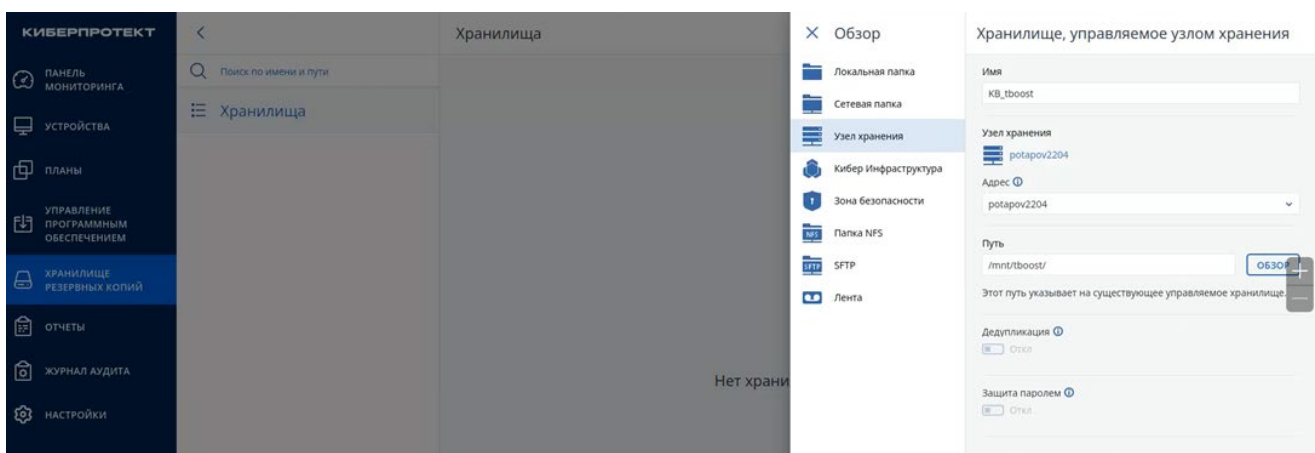
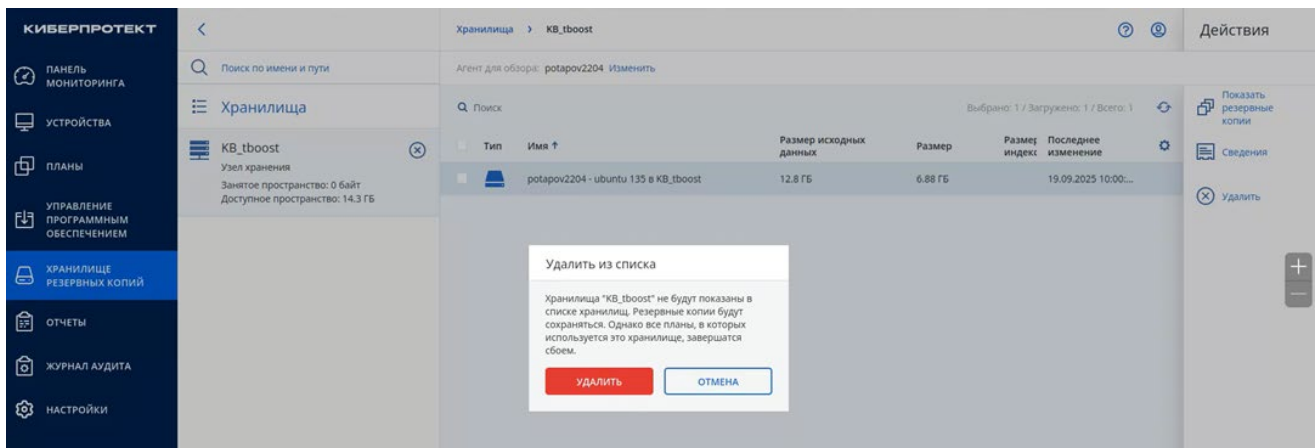
Результат: копия появилась:



9. Восстановление файла для проверки резервной копии:



10. Удаление смонитрованного хранилища и перемонтирование директории:



ЗАКЛЮЧЕНИЕ

Проведенные испытания подтвердили, что механизм снапшотов в TATLIN.BACKUP обеспечивает:

- Высокую надежность — точки восстановления создаются корректно и сохраняют неизменность данных.
- Оперативное восстановление — монтирование снапшота и возврат к ранее зафиксированному состоянию занимает минимальное время, что сводит простой системы к нулю.
- Сохранение целостности — в ходе тестирования после удаления и искажения исходных файлов все данные были успешно восстановлены без потерь и искажений.

Результаты подтверждают, что TATLIN.BACKUP эффективно защищает данные и обеспечивает мгновенное восстановление даже в условиях инцидентов и потерь на уровне хранилищ, включая последствия атак шифровальщиков, порчи и утраты данных резервного копирования.

Регулярное автоматическое создание снапшотов рекомендуется включать в стратегию резервного копирования для всех критических VFS.

В настоящее время ведется работа по интеграции управления снапшотами с ПО резервного копирования, что позволит расширить возможности системы.

Такая интеграция усилит связность процессов защиты данных и создаст основу для более устойчивой и управляемой инфраструктуры резервного копирования.