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.

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.

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

ОГЛАВЛЕНИЕ

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 снапшотах 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 (снапшотов), который будет подробно рассмотрен в следующих разделах.

	ВЕРСИИ ИСПОЛЬЗУЕМОГО 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 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 удаляется 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 снапшотов.
Для всех уровней действует общее правило: снапшот автоматически удаляется по истечении заданного срока хранения. Ручное изменение или удаление снапшота определяется уровнем защиты и ролевой моделью доступа.

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

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

Создание расписания снапшотов
Расписание снапшотов 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 — снапшоты будут создаваться автоматически в заданные интервалы.

Автоматическое устаревание
TATLIN.BACKUP поддерживает механизм «устаревания» снапшотов: 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 снапшоты за последние N дней, без накопления устаревших данных в хранилище;
- предсказуемое и контролируемое использование дискового пространства за счет автоматического удаления снапшотов 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 снапшотов;
- применение снапшотов 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 снапшоты 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, снапшоты 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 снапшотов в среде резервного копирования TATLIN.BACKUP 1.3.x, Кибер Бэкап 18.x.

Цель тестирования — подтвердить корректность, стабильность и предсказуемость работы функций снапшотов и восстановления данных.

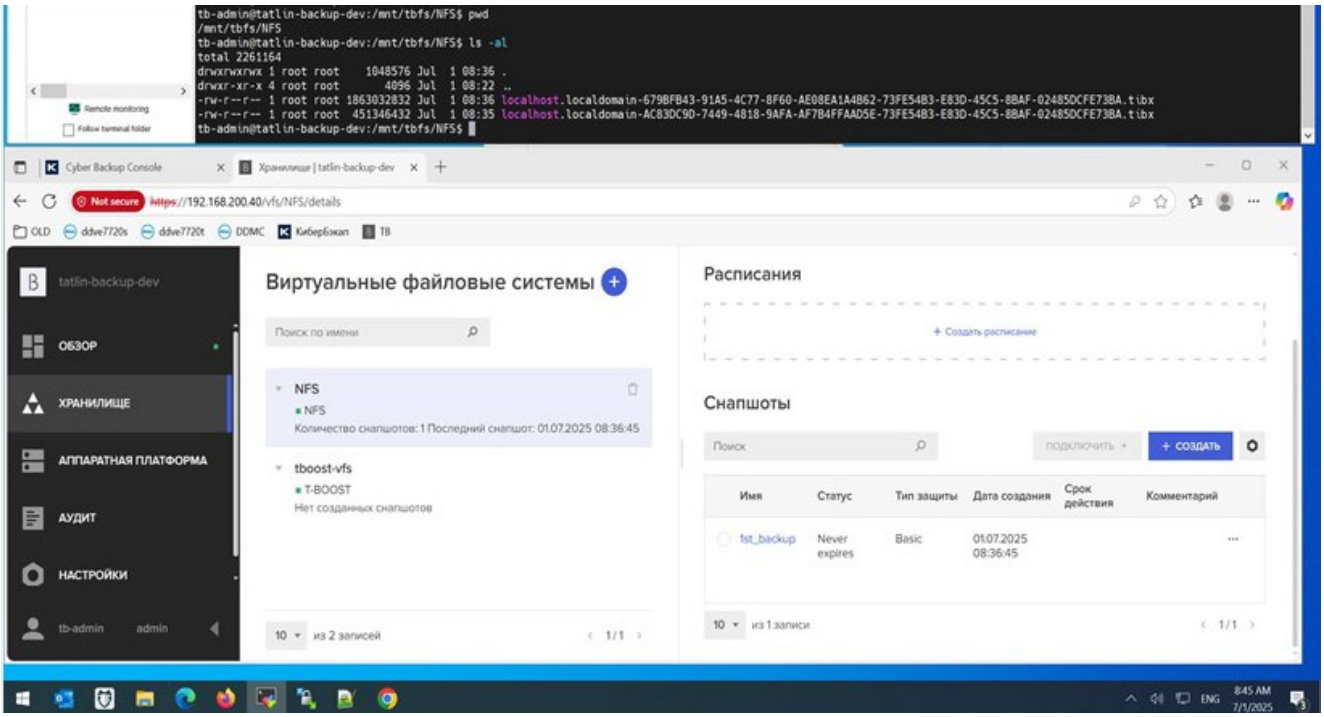
Проверяется механизм создания снапшотов в TATLIN.BACKUP, целостность и возможность восстановления данных после удаления или повреждения оригинальных файлов:

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

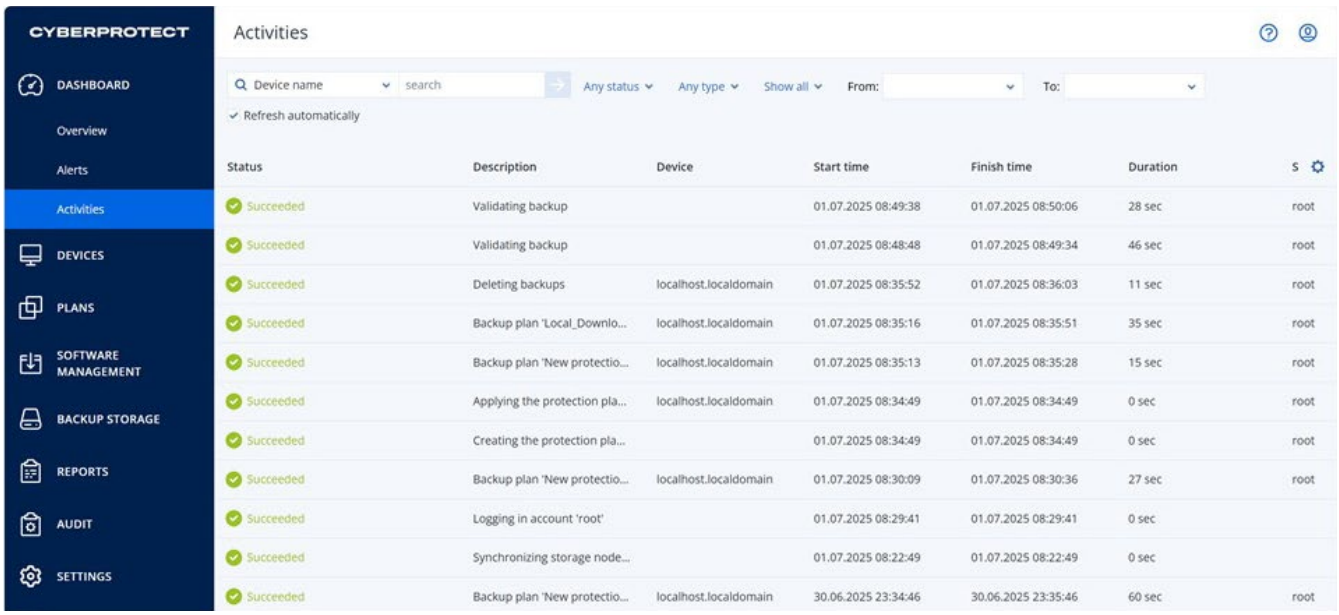
В ходе тестирования оба сценария восстановления — восстановление данных на уровне хранилища и восстановление через экспорт снапшота — были успешно выполнены с использованием соответствующих снапшотов без потери целостности данных и дополнительных задержек. Подтверждено, что механизм снапшотов TATLIN.BACKUP можно использовать не только для полного восстановления данных, но и для оперативного доступа к ним непосредственно из снапшота. Созданные снапшоты 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:



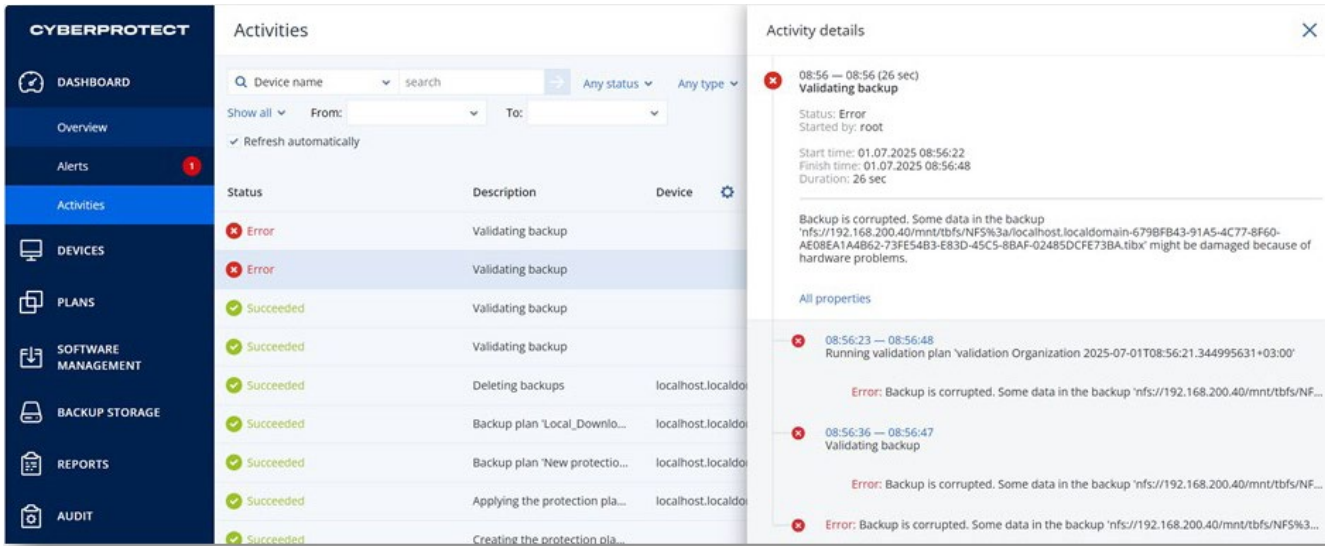
2. Прохождение валидации резервных копий:



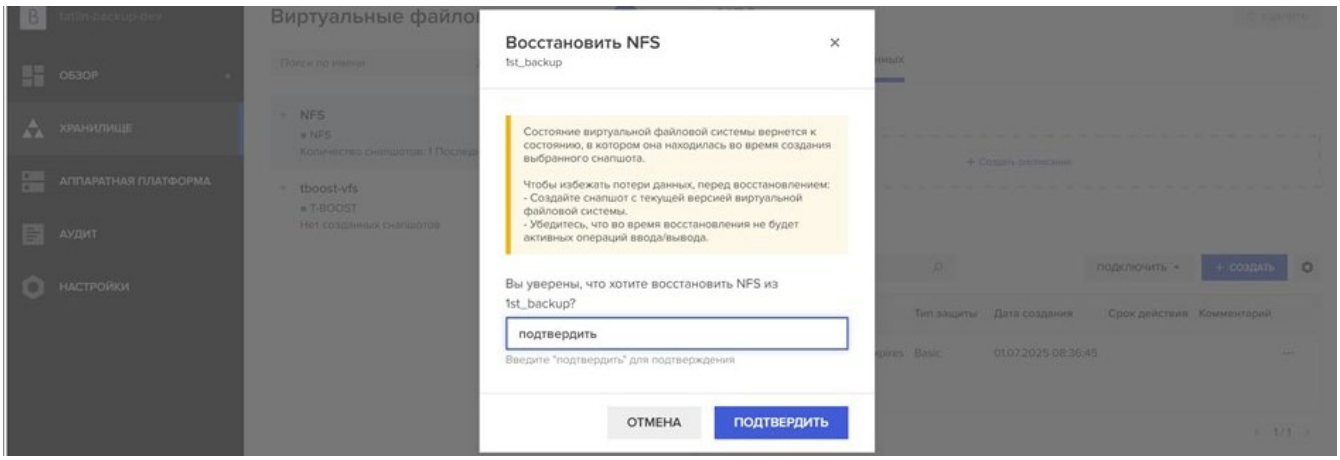
3. Эмуляция работы шифровальщика или недобросовестного персонала: перезапись файлов и проверка контрольных сумм:

```
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
-rw-r--r-- 1 root root  451346432 Jul  1 08:35 localhost.localdomain-AC83DCD9-7449-4818-9AFA-AF784FFAAD5E-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
17fdcfe06a842b672fadc0029505b1c6  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#
```

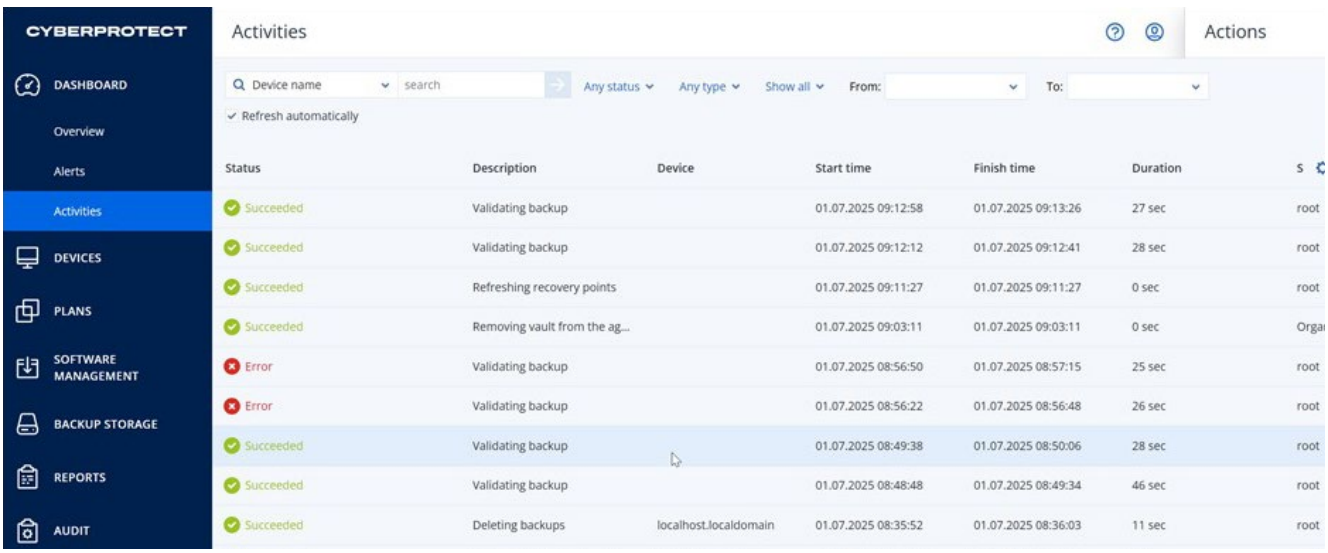
4. Повторная валидация резервных копий.
   Результат: валидация не пройдена:



5. Восстановление VFS из снапшота на TATLIN.BACKUP:

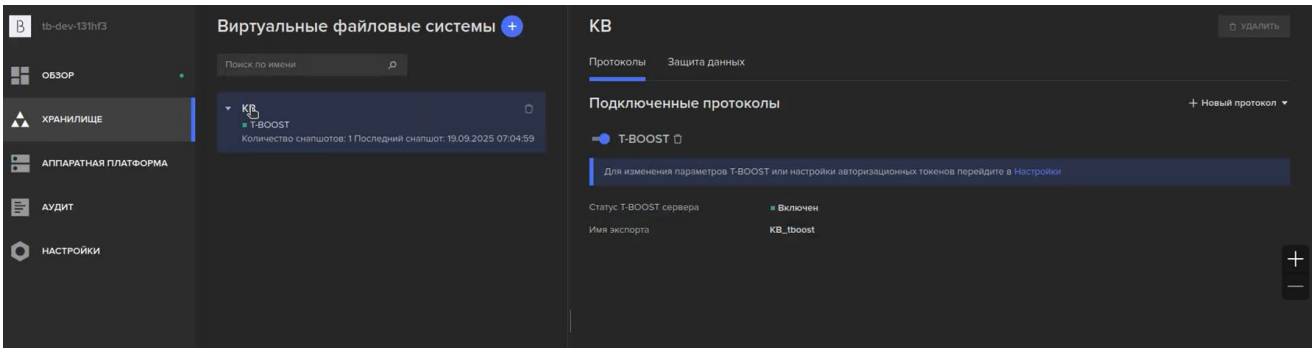


6. Проверка целостности данных после восстановления.
   Результат: проверка пройдена успешно:

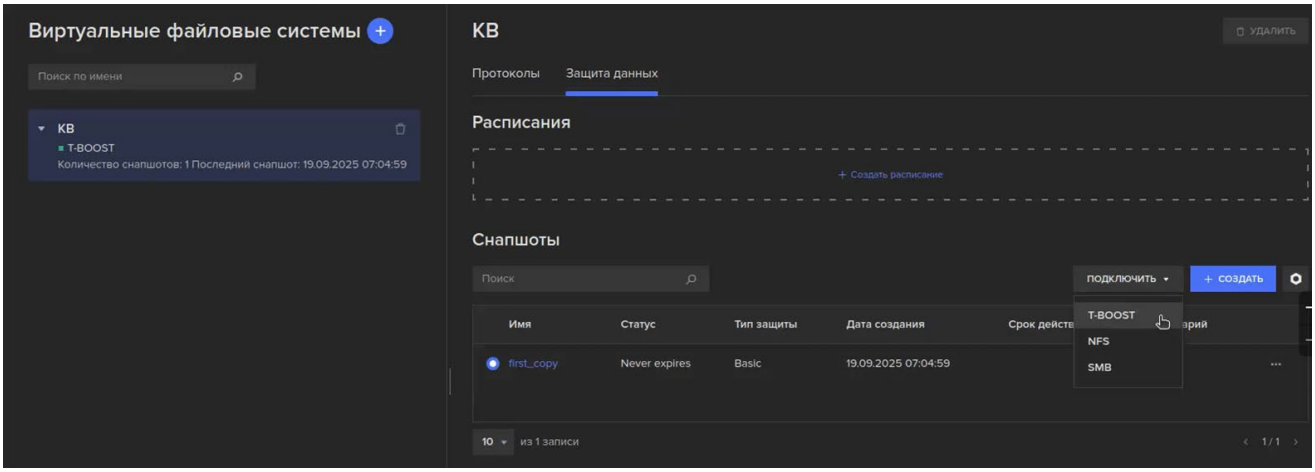


Восстановление через экспорт снапшота

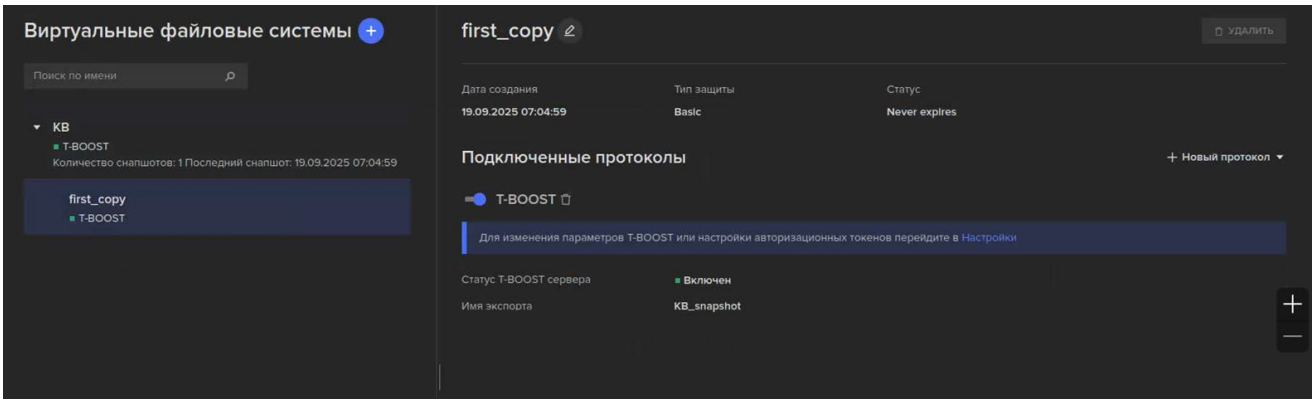
1. Создание снапшота на TATLIN.BACKUP:



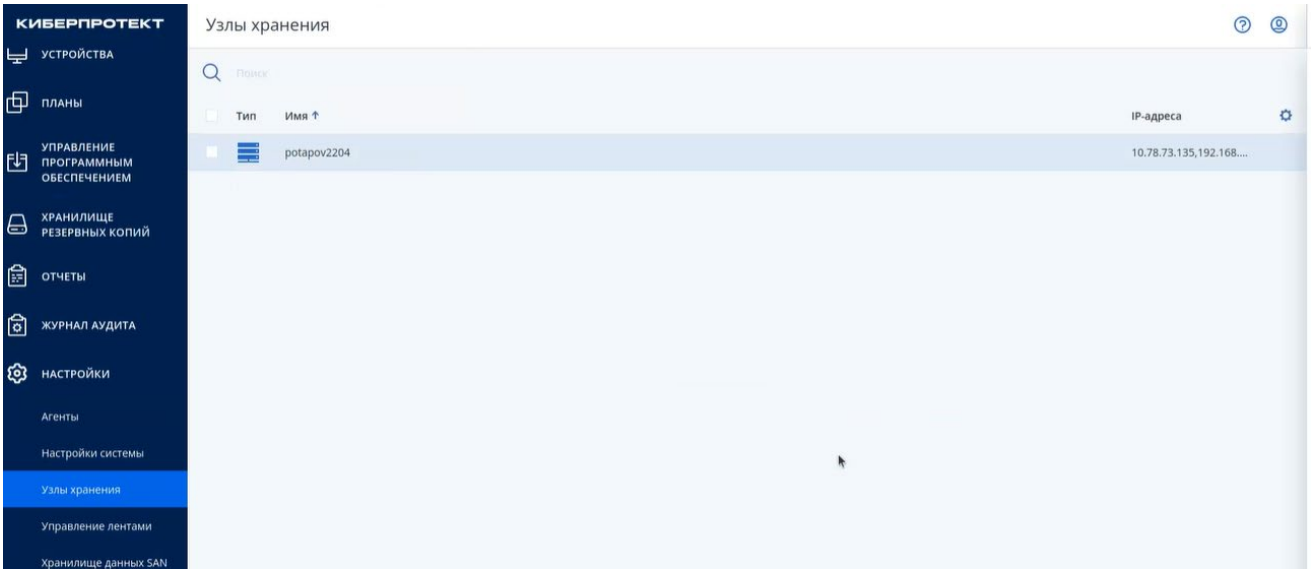
2. Экспорт снапшота по выбранному протоколу (в данном случае T-BOOST):



3. Проверка наличия экспорта:



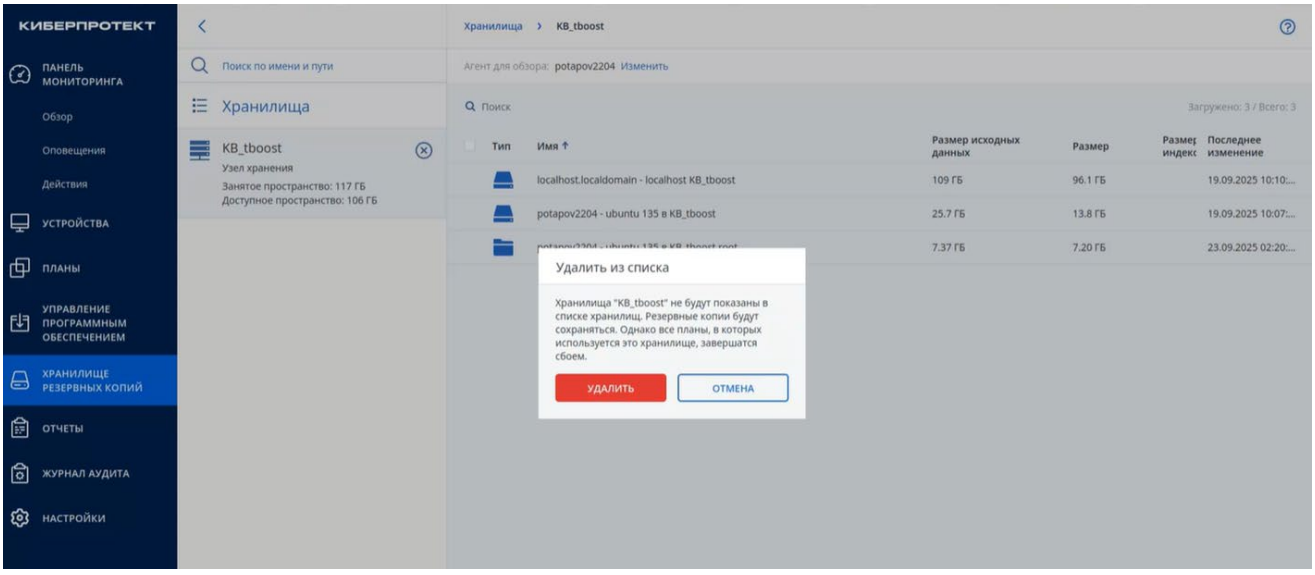
4. Создание временной директории.
   Чтобы работать со снапшотом хранилища, потребовалось обеспечить доступ к метаданным в режиме «чтение + запись»:
   a. Подключиться к узлу хранения по SSH.
   b. Создать временную директорию, в которую будет сохранен снапшот метаданных хранилища резервных копий:



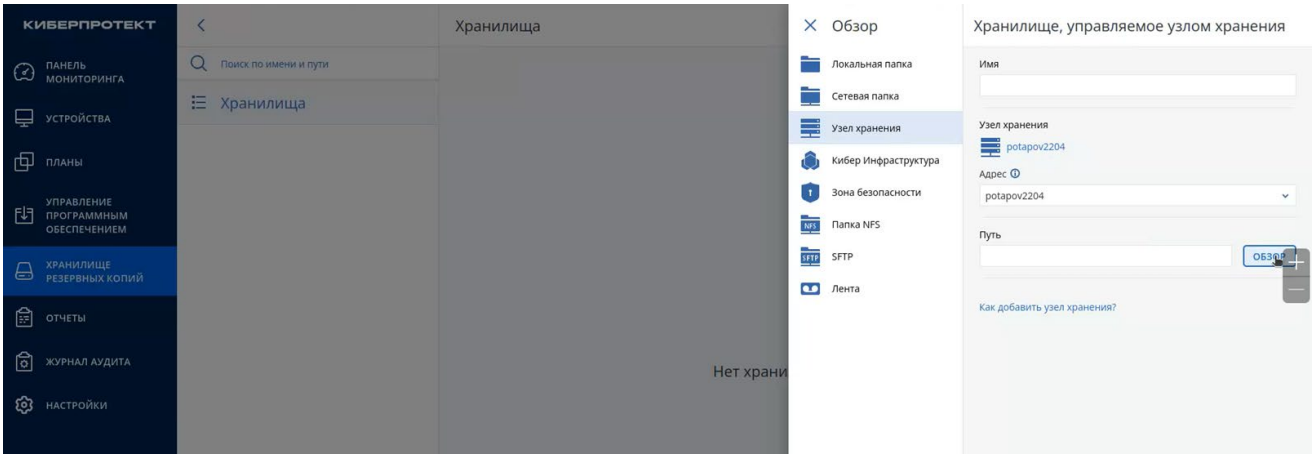
   c. Создать символьную ссылку на директорию с архивами резервных копий:

```
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#
```

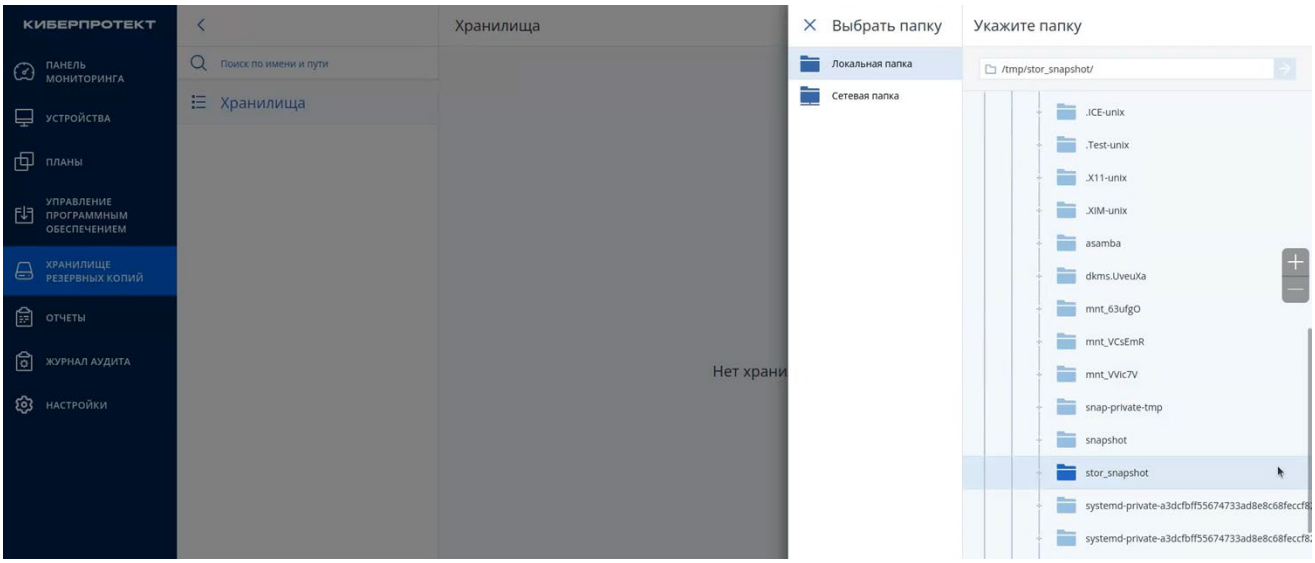
5. Удаление хранилища, выбранного под восстановление из снапшота:



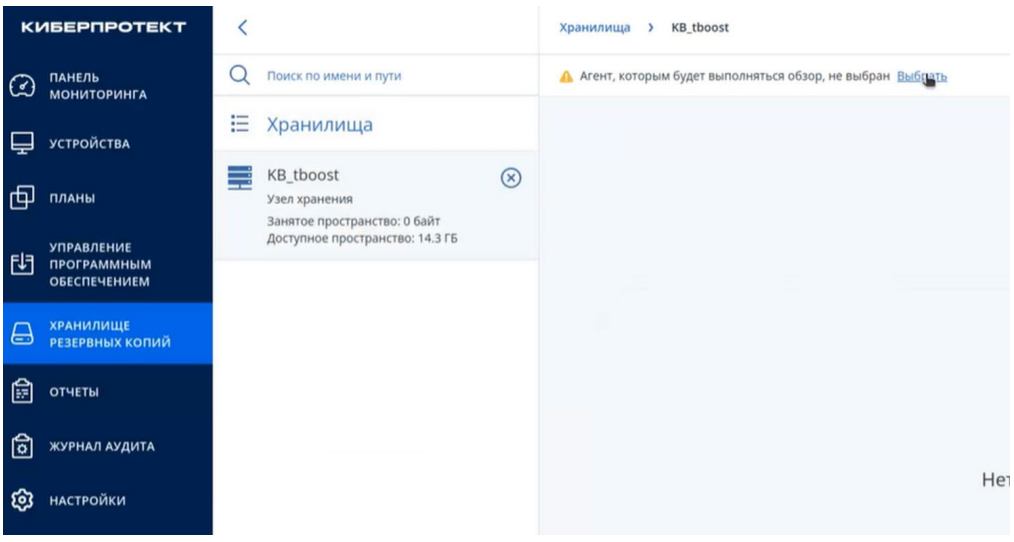
6. Создание хранилища в Кибер Бэкап:



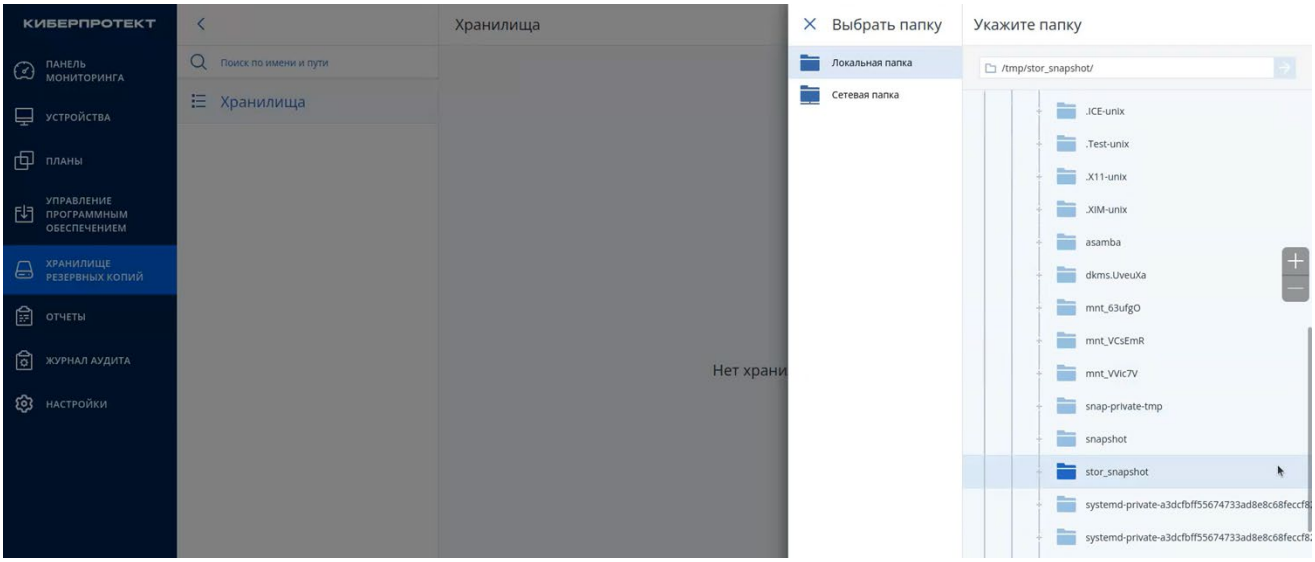
7. Выбор директории с импортированным снапшотом:



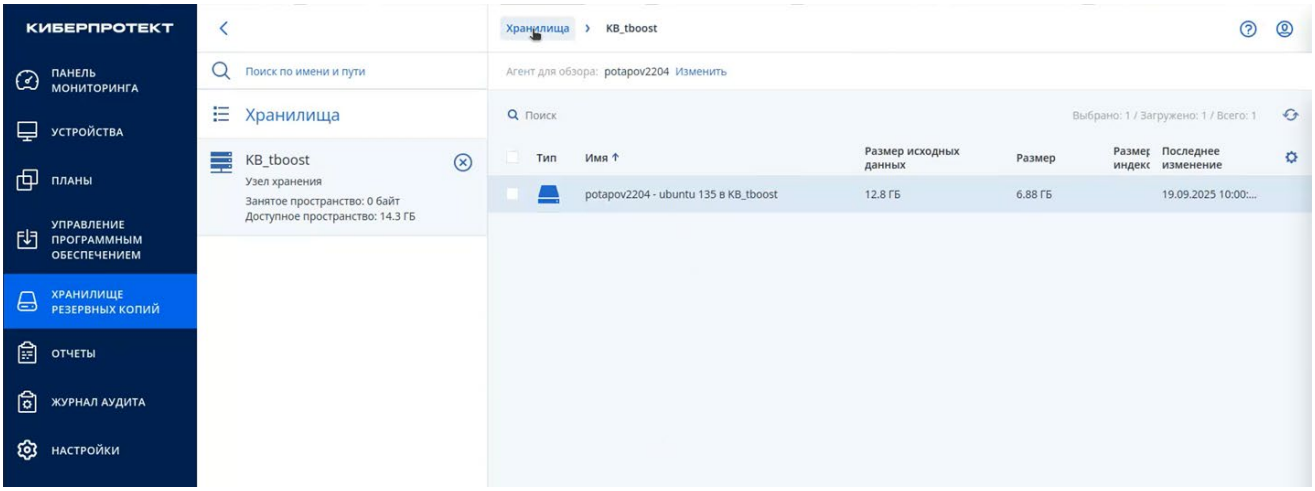
8. Выбор агента:

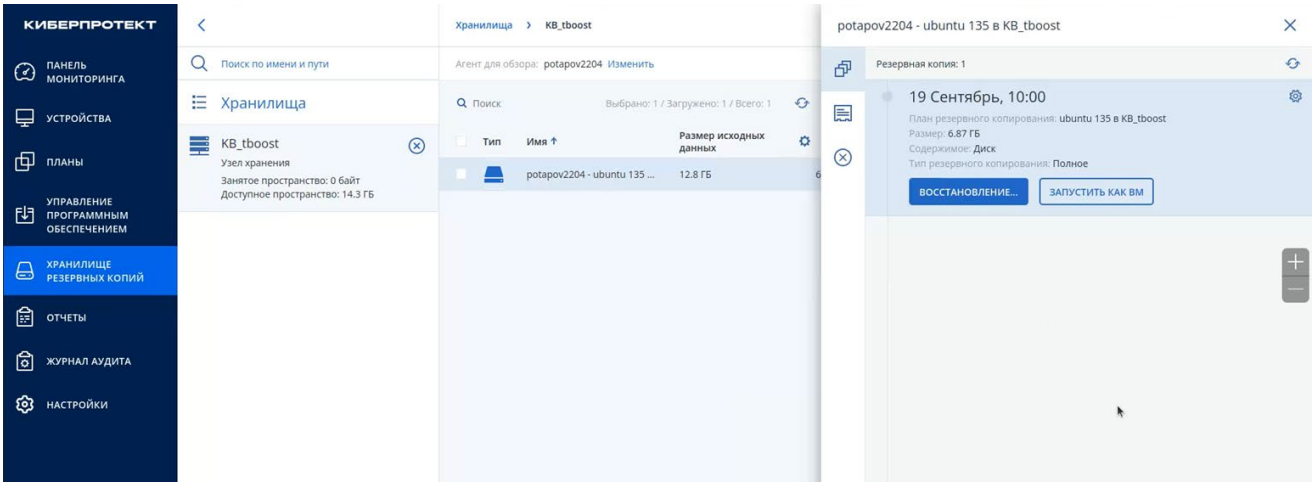


9. Выбор узла хранения, указанного при создании хранилища:

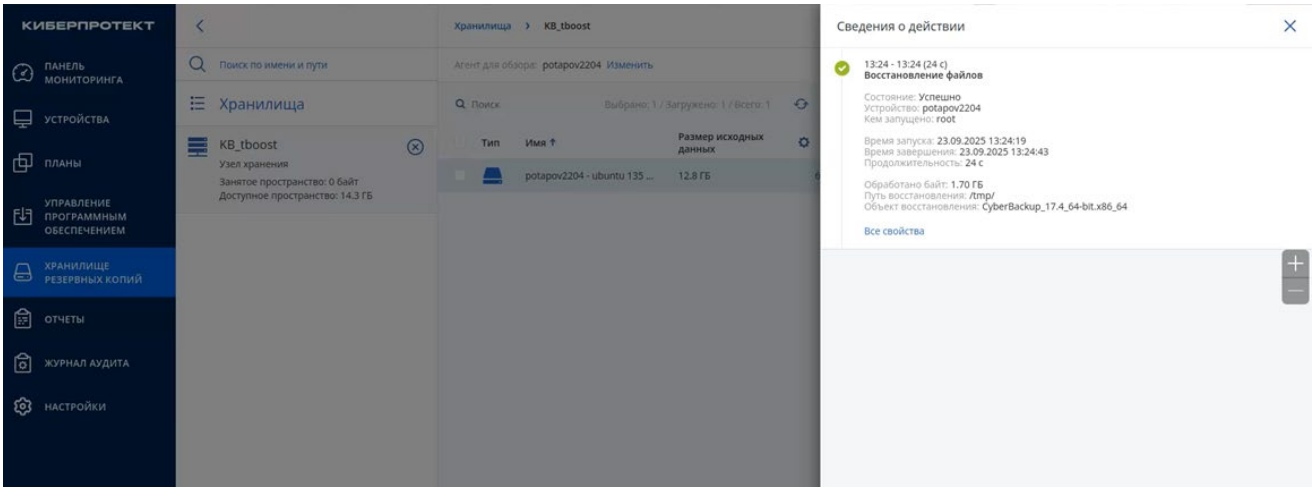


Результат: копия появилась:

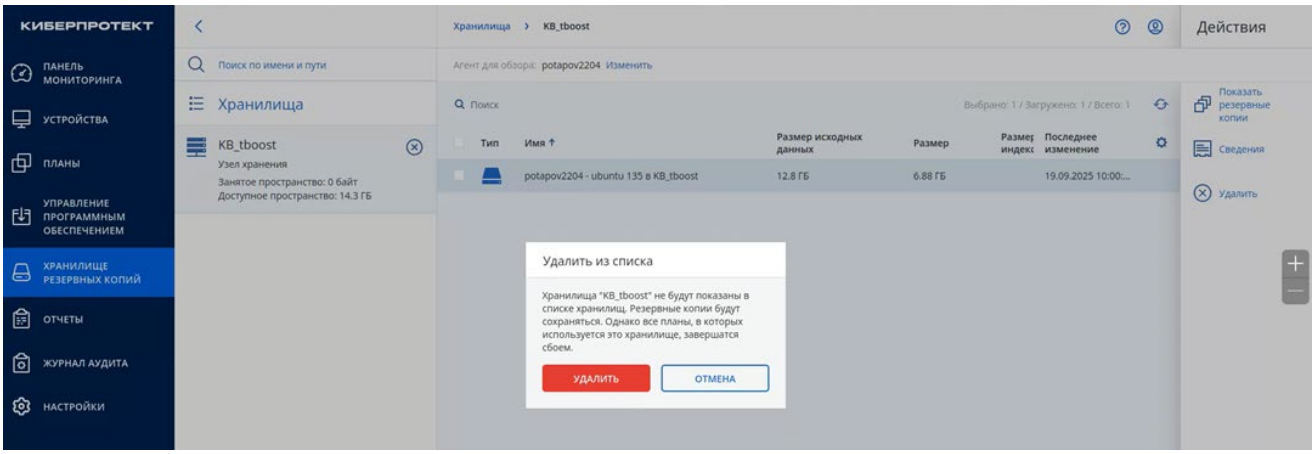


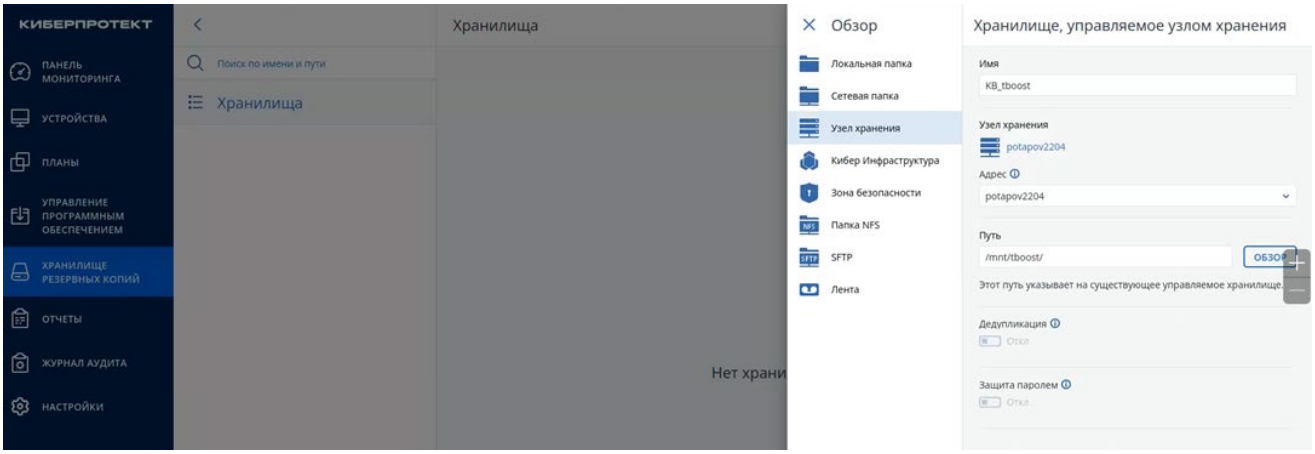


9. Восстановление файла для проверки резервной копии:



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.