УДК 004.056.5

Морозов Илья Михайлович сотрудник кафедры безопасности информационных технологий РГУ нефти и газа (НИУ) имени И.М. Губкина Россия, г. Москва

Иноземцева Кира Константиновна студентка

3 курс, РГУ нефти и газа (НИУ) имени И. М. Губкина

Россия, г. Москва

НАСТРОЙКА И ФУНКЦИОНАЛЬНОЕ ТЕСТИРОВАНИЕ VSS СЕРВЕРА НА БАЗЕ WINDOWS SERVER. ВОПРОСЫ БЕЗОПАСНОСТИ

Аннотация: Исследование посвящено комплексному анализу процесса настройки, функциональному тестированию и вопросам безопасности сервера на основе службы теневого копирования томов (Volume Shadow Copy Service – VSS) в операционной системе Windows Server 2022. В работе рассматриваются архитектурные компоненты VSS, этапы ее развертывания в изолированной среде виртуализации Oracle VirtualBox и ключевые механизмы обеспечения безопасности: разграничение прав доступа, аудит операций и защита точек восстановления. Экспериментальная часть включает пошаговую настройку VSS, создание теневых копий, моделирование инцидента удаления данных и процедуру восстановления. Особое внимание уделено анализу встроенных средств аудита и проверке модели разграничения привилегий между рядовыми пользователями и администраторами. Результаты подтверждают, что грамотно настроенная служба VSS является эффективным, надежным и безопасным инструментом оперативного восстановления данных, критически важным для обеспечения отказоустойчивости ИТ-инфраструктуры.

Ключевые слова: VSS, теневое копирование, Windows Server, восстановление данных, сетевое хранилище, резервное копирование.

Annotation: *This study is devoted to a comprehensive analysis of the setup process, functional testing, and security aspects of a server based on the Volume Shadow Copy Service (VSS) in the Windows Server 2022 operating system. The paper examines the architectural components of VSS, the stages of its deployment in an isolated Oracle VirtualBox virtualization environment, and key security mechanisms: access control, operation auditing, and recovery point protection. The experimental part includes step-by-step VSS configuration, creation of shadow copies, simulation of a data deletion incident, and the recovery procedure. Particular attention is paid to the analysis of built-in audit tools and verification of the privilege separation model between regular users and administrators. The results confirm that a properly configured VSS service is an effective, reliable, and secure tool for operational data recovery, which is critically important for ensuring the fault tolerance of IT infrastructure.*

Keywords: *VSS, shadow copy, Windows Server, data recovery, network storage, backup.*

РАЗДЕЛ 1. ВВЕДЕНИЕ

Актуальность: В современной цифровой экономике данные являются ключевым стратегическим активом, а их потеря несет прямые финансовые и репутационные риски. Согласно глобальному исследованию инцидентов информационной безопасности (DBIR), эксплуатация уязвимостей и человеческий фактор остаются одними из основных причин утечек и повреждения данных [1]. Особую угрозу представляют атаки программ-шифровальщиков (ransomware), которые в 2022–2023 годах активно совершенствовали тактики, целенаправленно нацеливаясь на удаление или повреждение точек восстановления, включая теневые копии VSS, чтобы затруднить восстановление без выплаты выкупа [3]. В этих условиях критически важной задачей становится не только наличие систем резервного

копирования, но и обеспечение их отказоустойчивости и безопасности. Встроенная в Windows Server служба теневого копирования томов (Volume Shadow Copy Service, VSS) представляет собой фундаментальный, предоставляемый на уровне операционной системы, механизм создания согласованных моментальных снимков (снапшотов) данных [5]. Ее грамотная настройка и защита позволяют организовать быстрое восстановление информации после случайного удаления, повреждения или в результате кибератаки, что напрямую влияет на непрерывность бизнес-процессов.

Объект исследования: Процесс обеспечения отказоустойчивости и восстановления данных в информационных системах под управлением операционной системы Windows Server.

Предмет исследования: Механизм работы, настройка и функциональное тестирование службы теневого копирования томов (Volume Shadow Copy Service) с учетом аспектов информационной безопасности в изолированной среде виртуализации.

Цель исследования: На основе анализа уязвимостей и угроз безопасности VSS разработать и практически проверить комплекс мер, обеспечивающих защиту точек восстановления от компрометации и несанкционированного удаления в среде Windows Server.

РАЗДЕЛ 2. ОБЗОР ЛИТЕРАТУРЫ И МЕТОДОЛОГИЯ ИССЕЛЕДОВАНИЯ

Технология теневого копирования томов (VSS) является критически важным компонентом инфраструктуры резервного копирования в экосистеме Microsoft Windows. Целью настоящего обзора является не повторение общеизвестных архитектурных принципов (таких как модель взаимодействия VSS Requestor, Writer и Provider), которые детально документированы в официальных источниках корпорации Microsoft[5] и учебных пособиях по

системному администрированию[9], а выявление пробелов в существующих подходах и обоснование направленности данного исследования.

Анализ доступной литературы и документации позволяет выделить два основных подхода к рассмотрению VSS:

1) Процедурно-описательный подход, характерный для официальных руководств[5] и технических заметок вендоров[2]. Эти источники фокусируются на корректной последовательности шагов развертывания, конфигурации хранилища и устранении типовых ошибок. Их ценность заключается в предоставлении проверенных методик, однако вопросы проактивной безопасности, анализа уязвимостей и моделирования угроз остаются на периферии или не рассматриваются вовсе.
2) Контекстно-ориентированный подход, представленный в учебно-методической литературе по защите информации и обеспечению непрерывности бизнеса[9]. Данные работы рассматривают VSS как элемент общей стратегии резервного копирования, подчеркивая ее роль в оперативном восстановлении. Тем не менее, конкретные, технически обоснованные рекомендации по защите именно этой службы от целевых атак (например, со стороны ransomware) зачастую носят общий характер.

Таким образом, обнаруживается существенный пробел: между инструкцией по настройке (как включить) и высокоуровневой стратегией (зачем нужно) отсутствует практико-ориентированный анализ безопасности (как защитить). Большинство руководств не дают системного ответа на ключевые вопросы:

- Каков спектр актуальных уязвимостей (CVE) конкретно для компонентов VSS и как они были устранены?
- Какие настройки, помимо базовых, необходимы для обеспечения подотчетности (аудита) операций с тенями?

- Как встроенная модель безопасности VSS соотносится с реальными тактиками злоумышленников, целенаправленно атакующих инфраструктуру резервного копирования?

Методологической основой данного исследования является синтез двух подходов: строгое следование проверенным процедурам настройки в соответствии с рекомендациями[5,9] и их критическое развитие за счет интеграции принципов безопасной конфигурации и анализа угроз. Исследование направлено на заполнение указанного пробела путем перехода от описания функциональности к разработке и практической проверке мер по обеспечению защиты VSS-инфраструктуры.

Вопросы безопасности VSS: угрозы и уязвимости

Безопасность инфраструктуры VSS подвергается рискам как со стороны внешних атак, так и из-за внутренних недостатков конфигурации. Анализ реестра уязвимостей (CVE) и отчетов о киберугрозах позволяет систематизировать ключевые угрозы и оценить эффективность стандартных мер защиты.

1. Критические уязвимости компонентов VSS: Наиболее опасными являются уязвимости, позволяющие злоумышленнику напрямую нарушить работу службы или получить над ней контроль. В таблице 1 представлен анализ характерных уязвимостей, затрагивающих стек VSS и связанный драйвер volsnap.sys.

Таблица 1.

Анализ актуальных уязвимостей (CVE), связанных с VSS и volsnap.sys

Идентификатор CVE	Дата публикации	Уровень опасности (CVSS)	Краткое описание воздействия	Вектор атаки / Необходимые привилегии	Статус и рекомендуемые меры
CVE-2021-28316	апр.21	7.8 (HIGH)	Неверное обращение с объектами в памяти драйвером volsnap.sys. Позволяет локальному пользователю повысить привилегии до уровня SYSTEM.	Локальный / Наличие учётной записи пользователя	Закрыта. Требуется установка обновления безопасности KB5001330. Подчёркивает критическую важность регулярного обновления ОС.
CVE-2022-37989	сен.22	7.8 (HIGH)	Уязвимость проверки подлинности в Windows Kerberos. Может использоваться для получения прав администратора в домене, что косвенно открывает доступ к управлению VSS на всех серверах.	Сетевой / Учётная запись пользователя домена	Закрыта. Устраняется обновлениями за сентябрь 2022 г. Демонстрирует, что безопасность VSS зависит от общей инфраструктуры безопасности (Kerberos, Active Directory).
CVE-2023-28252	апр.23	7.8 (HIGH)	Уязвимость в драйвере файловой системы CLFS.sys. Приводит к повышению привилегий, что позволяет получить права для выполнения команд управления VSS (например, vssadmin delete shadows).	Локальный / Наличие учётной записи пользователя	Закрыта. Устраняется последними обновлениями. Показывает, как уязвимости в смежных компонентах ОС могут быть использованы для атаки на механизмы восстановления.

Уязвимости, затрагивающие VSS, носят преимущественно локальный характер и направлены на повышение привилегий (Elevation of Privilege, EoP). Их успешная эксплуатация превращает обычного пользователя в администратора, снимая ключевую встроенную защиту VSS. Единственной

гарантированной мерой противодействия является своевременная установка всех обновлений безопасности Windows.

2. Целевые атаки на инфраструктуру восстановления: Помимо эксплуатации «классических» уязвимостей, злоумышленники применяют целенаправленные тактики против механизмов резервного копирования. Ключевой из них является принудительное удаление теневых копий.

- Механизм: Используя скомпрометированные учётные записи администраторов или эксплуатируя уязвимости для повышения прав, вредоносное ПО (например, ransomware семейства Ryuk, Conti) выполняет команды vssadmin delete shadows /all или wbadmin delete catalog.
- Цель**:** Безвозвратно уничтожить точки восстановления, чтобы сделать невозможным восстановление файлов без оплаты выкупа[3].
- Анализ защиты: Данная тактика не является эксплуатацией уязвимости ПО, а представляет собой злоупотребление легитимными функциями. Стандартная модель разграничения прав VSS эффективна против неадминистратора, но бесполезна при компрометации учётной записи с правами администратора.

3. Недостатки конфигурации и аудита по умолчанию:

- Отсутствие детального аудита: Конфигурация Windows по умолчанию не отслеживает операции с конкретными объектами теневых копий. Без включения политики Audit Other Object Access Events в журналах безопасности невозможно установить, кто, когда и какую именно теневую копию удалил или изменил. Это исключает возможность расследования инцидента.
- Зависимость от модели прав Windows: Вся защита VSS построена на разграничении прав Windows. Следовательно, её эффективность напрямую зависит от общей гигиены безопасности: стойкости паролей,

использования многофакторной аутентификации для администраторов и соблюдения принципа наименьших привилегий.

Методы исследования

Процедура настройки и тестирования базируется на официальных рекомендациях Microsoft по развертыванию VSS[5] и лучших практиках безопасного администрирования, изложенных в учебной литературе[9]. Данный подход обеспечивает соответствие стандартным процедурам при интеграции в них аспектов безопасности.

Тип исследования: Данная работа представляет собой прикладное экспериментальное исследование. Его целью является практическая проверка функциональности, надёжности и безопасности стандартного инструментария VSS в контролируемых условиях с последующей выработкой рекомендаций для системных администраторов.

Характеристика среды исследования: Эксперимент проводился в изолированной среде виртуализации (Oracle VirtualBox), что соответствует методологии безопасного тестирования. Конфигурация виртуальной машины (Windows Server 2022, 4 ГБ ОЗУ, отдельный диск для данных) была подобрана для адекватного моделирования рабочей среды файлового сервера малого или среднего предприятия, где развертывание VSS наиболее типично.

Процедура проведения исследования:

Исследование проводилось в три последовательных этапа:

1. **Этап анализа и проектирования мер защиты:**
   - Анализ документации[5,9] и актуальных уязвимостей (CVE) для выявления ключевых угроз безопасности VSS (см. Таблицу 1).
   - На основе анализа определены проверяемые меры защиты: строгое разграничение прав (роли

администратор/пользователь) и необходимость настройки расширенного аудита.

2. **Этап реализации и функционально-безопасностного тестирования:**

- Стандартное развертывание и настройка VSS в соответствии с [5].
- Функциональное тестирование: Проверка рабочего цикла «создание-восстановление» данных.
- Тестирование эффективности мер защиты:

    a. *Проверка модели разграничения прав:* Попытка выполнения административных команд (vssadmin delete shadows) от имени пользователя без привилегий.

    b. *Проверка возможностей аудита:* Анализ журналов событий Windows на полноту регистрации действий с VSS при стандартной и расширенной настройке политик аудита.

    c. Моделирование инцидента удаления файла и восстановления из теневой копии.

3. **Аналитический этап:**

- Систематизация данных о работоспособности функций VSS и эффективности проверенных мер защиты.
- Формулировка выводов и конкретных практических рекомендаций по настройке безопасности VSS.

РАЗДЕЛ 3. ОСНОВНЫЕ МОМЕНТЫ ЭКСПЕРИМЕНТАЛЬНОГО ИССЛЕДОВАНИЯ

Эксперимент был направлен на практическую проверку мер защиты, выявленных в результате анализа уязвимостей (см. Таблицу 1, Раздел 2), а именно: эффективности встроенного разграничения прав и необходимости настройки расширенного аудита. Для проведения исследований была

развернута виртуальная среда на базе Oracle VirtualBox. Конфигурация виртуальной машины включала:

- Операционная система: Microsoft Windows Server 2022 Standard;
- Оперативная память: 4 ГБ;
- Процессор: 2 виртуальных ядра;
- Дисковая подсистема:

1) Диск 0: Системный раздел, 50 ГБ;

2) Диск 1: Раздел данных, 30 ГБ, файловая система NTFS.

На виртуальную машину были установлены роли File and Storage Services и File Server VSS Agent Service, необходимые для работы службы теневого копирования томов. На диске G:\ была создана тестовая файловая структура в папке TestData, содержащая документы различных форматов.

Перед началом тестирования была проверена работа службы VSS. Изначально служба находилась в состоянии Stopped, что потребовало её запуска и настройки автоматического запуска:

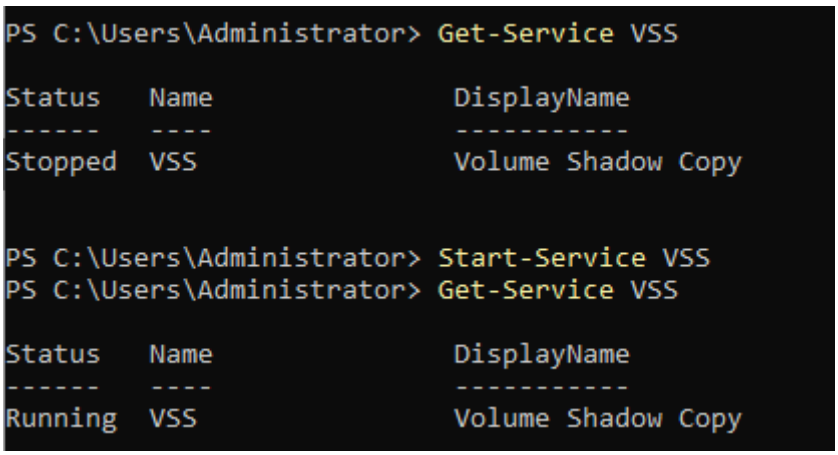

Рисунок 1. Просмотр состояния службы VSS

Для проверки доступных провайдеров VSS использована команда:

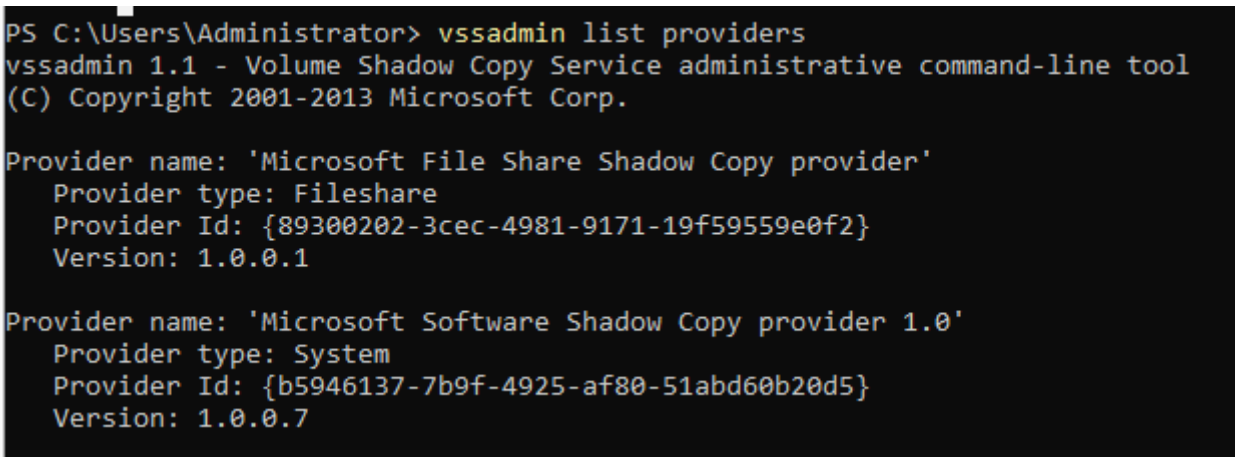

Рисунок 2. Просмотр провайдеров

Далее выполнена настройка хранилища теневых копий для тома G:\:

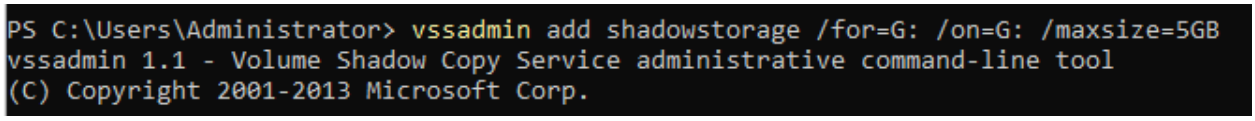

Рисунок 3. Настройка хранилища теневых копий

Успешность выполнения команды подтвердила возможность резервирования пространства под теневые копии.

Создание теневой копии выполнено командой:

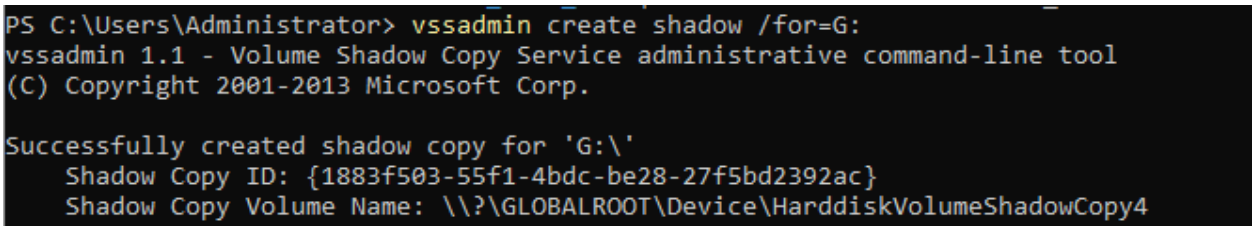

Рисунок 4. Создание теневой копии после добавления файлов в папку

После удаления тестового файла file_num2345678.txt восстановление выполнено через вкладку «Предыдущие версии» в свойствах папки G:\TestData. Интерфейс корректно отобразил доступные точки восстановления, что позволило вернуть удалённый файл.

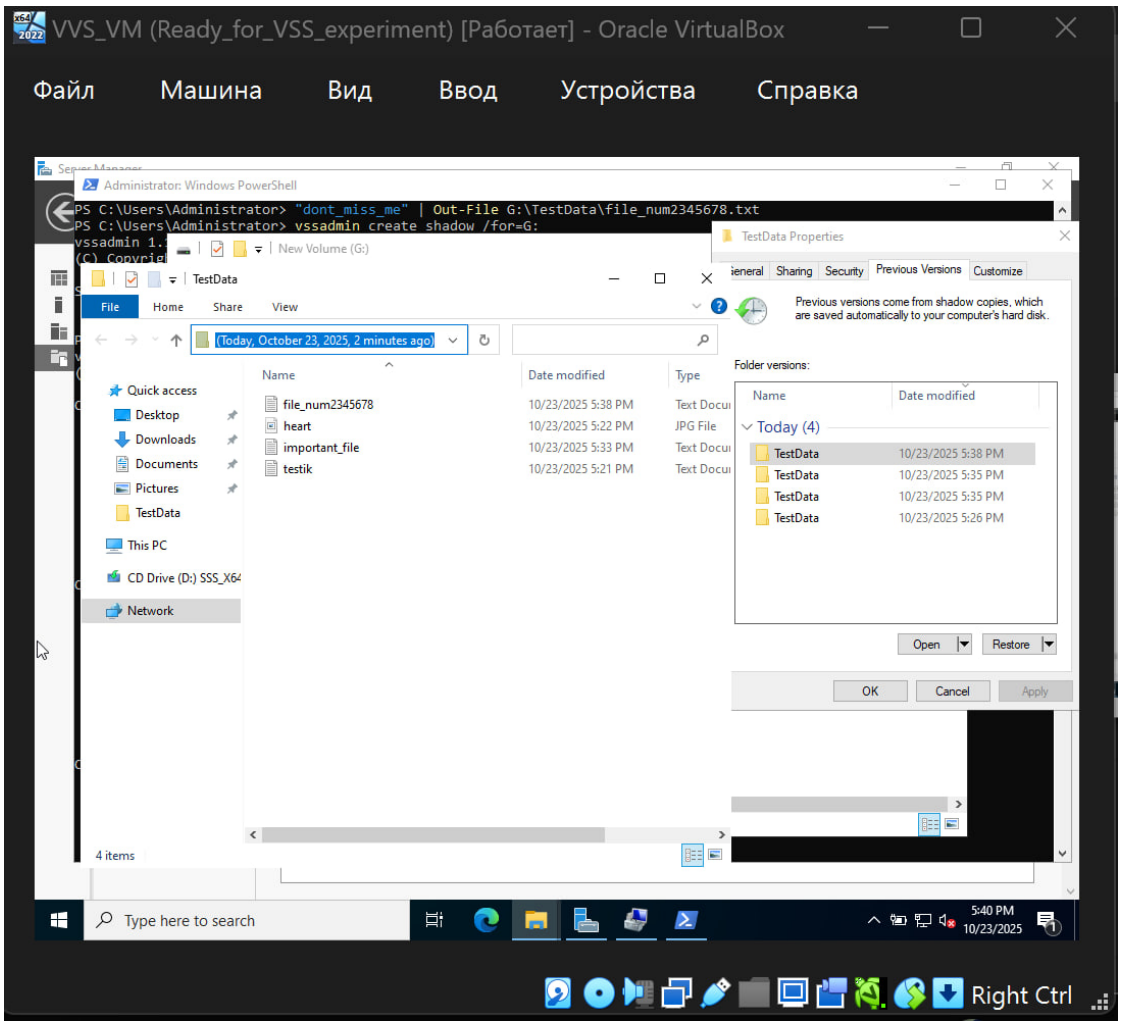

Рисунок 5. Просмотр теневой копии папки TestData

Анализ аспектов безопасности при работе с VSS:

В процессе исследования проанализирована запись событий, связанных с работой службы теневого копирования. Основные события VSS фиксируются в журнале **Application** с источниками VSS и volsnap.

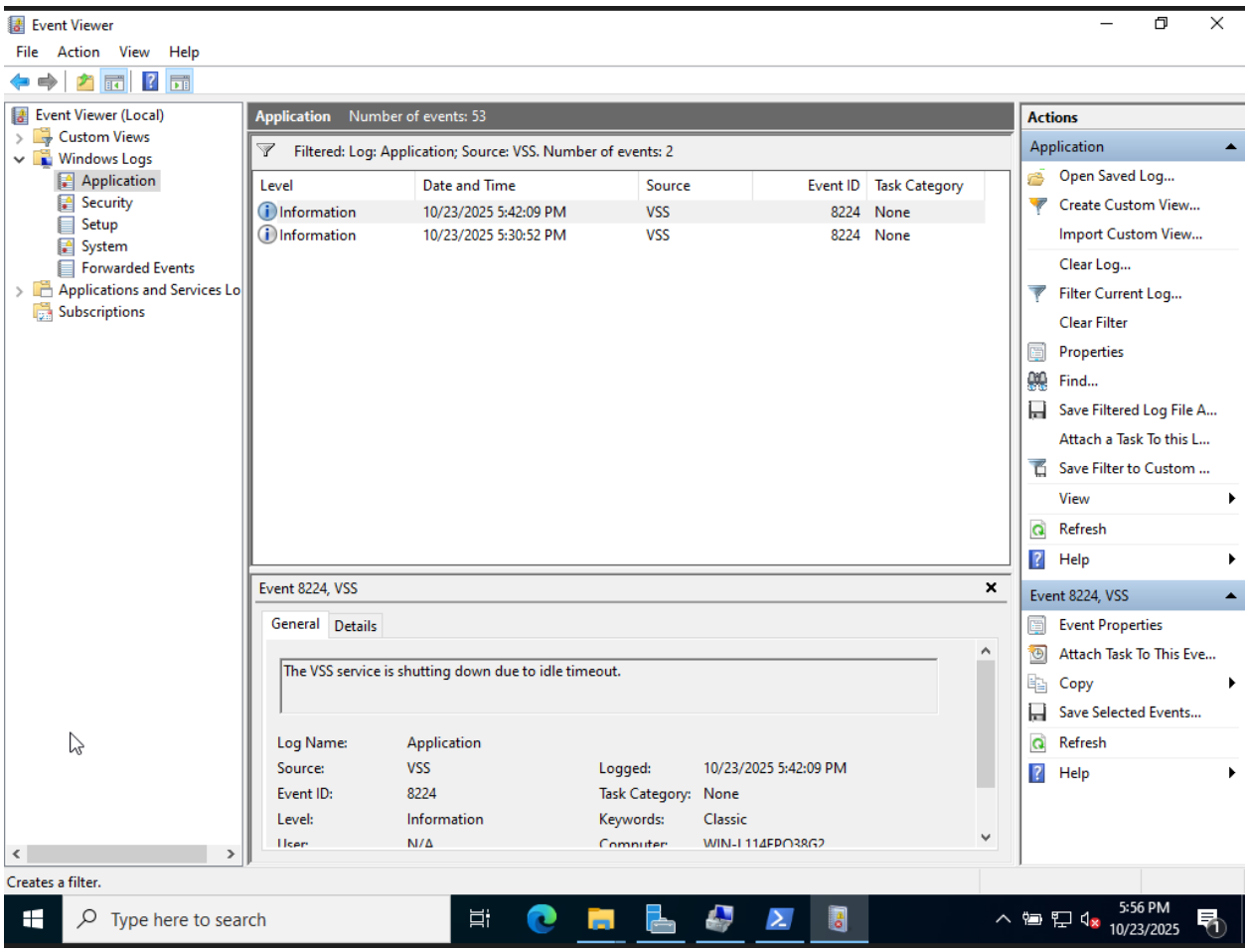

Рисунок 6. События службы VSS в журнале Application

Для детального аудита операций создания, удаления и изменения теневых копий требуется ручная активация соответствующих политик аудита в разделе: *Local Security Policy → Advanced Audit Policy Configuration → Object Access → Audit Other Object Access Events.* Что является необходимым условием для расследования инцидентов, связанных с удалением точек восстановления, например, в случае атаки ransomware или эксплуатации уязвимостей для повышения привилегий.

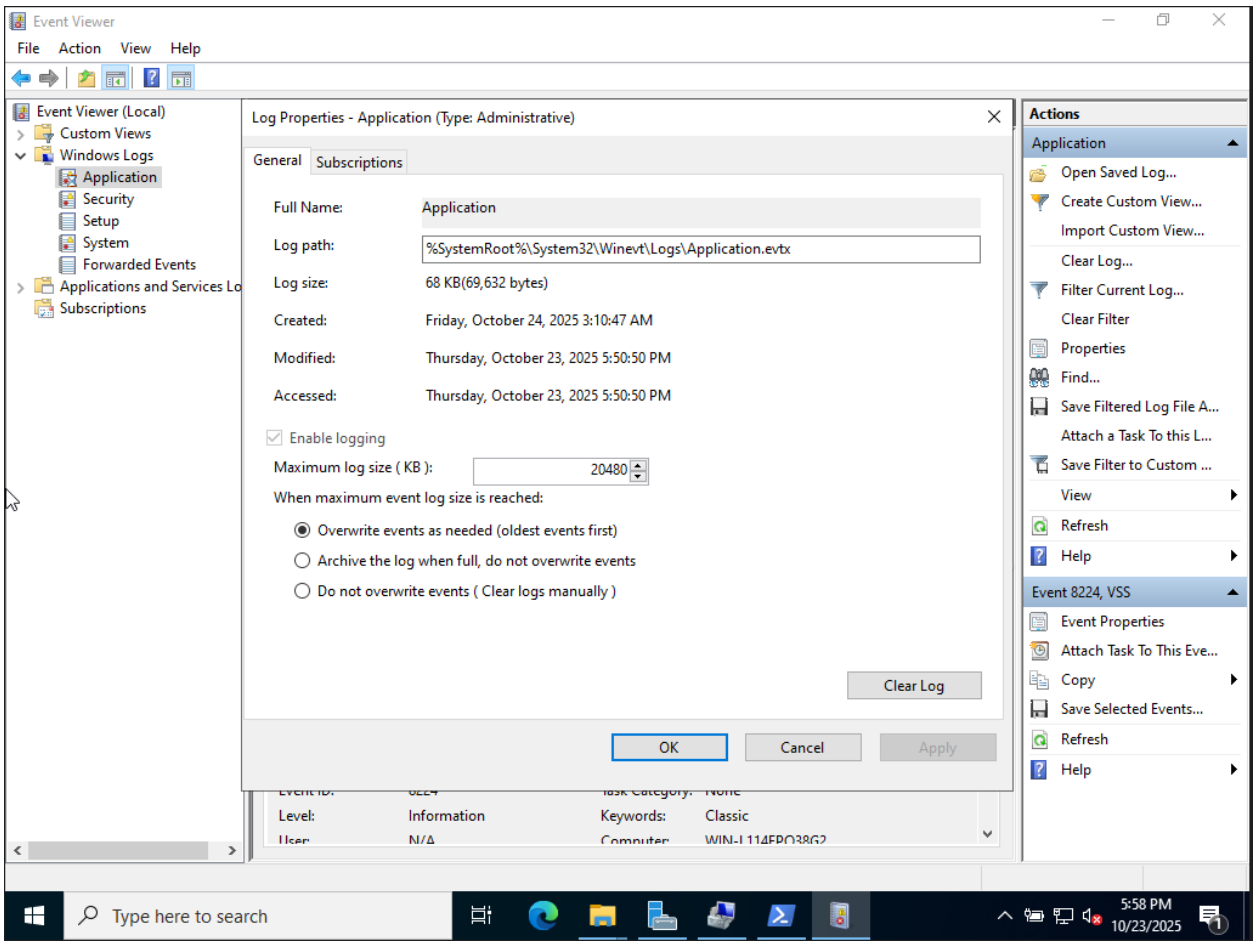

Рисунок 7. Свойства журнала Application с информацией о размере и датах событий

Анализ прав доступа к управлению тенями:

Экспериментально установлено, что для операций восстановления собственных файлов через оснастку «Предыдущие версии» пользователю требуются стандартные права на чтение файлов. Однако для выполнения административных задач, таких как:

- создание теневых копий с помощью vssadmin create shadow;
- удаление точек восстановления (vssadmin delete shadows);
- изменение параметров хранилища (vssadmin resize shadowstorage);

требуются права локального администратора. Это является важной встроенной мерой защиты, предотвращающей несанкционированное удаление

или изменение точек восстановления злоумышленником с правами обычного пользователя.

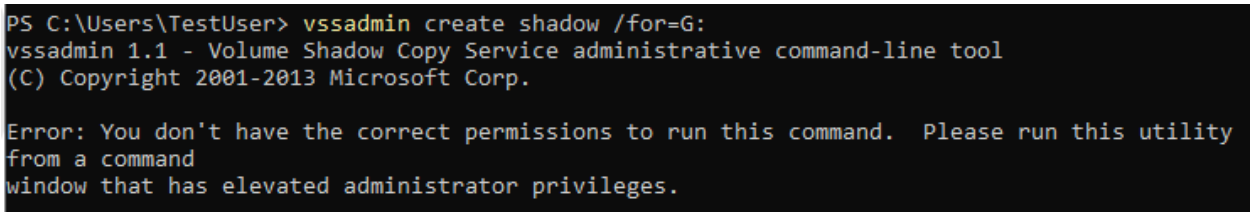

Рисунок 8. Анализ прав доступа к управлению тенями от имени обычного пользователя

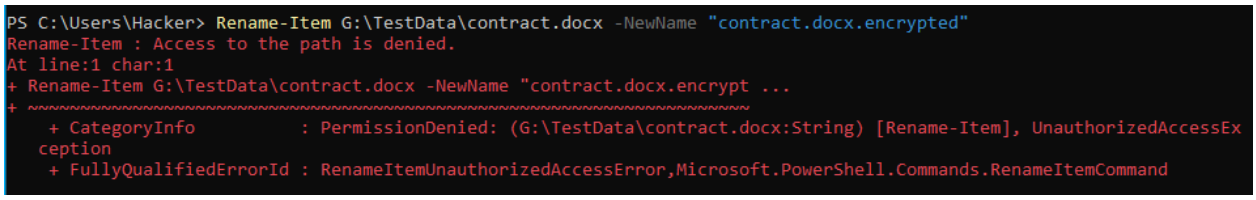

Рисунок 9. Анализ прав доступа к изменению названий файлов для дальнейшей попытки управления тенями

РАЗДЕЛ 4. РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Проведенное экспериментальное исследование позволило получить следующие практические результаты:

1. **Успешное развертывание и настройка.** В изолированной среде виртуализации успешно развернут и настроен VSS-сервер на базе Windows Server 2022, что подтверждает тиражируемость данной процедуры. Экспериментально подтверждена полная работоспособность ключевых функций VSS: создание теневых копий тома, хранение точек восстановления и восстановление данных через графический интерфейс «Предыдущие версии». Установлено, что процесс создания теневой копии выполняется быстро (в течение секунд)

и не требует остановки пользовательских приложений, что соответствует требованиям к оперативному восстановлению в продакшн-средах.

2. **Анализ встроенных механизмов безопасности и выявленные ограничения.** Модель безопасности VSS строго разделяет права конечных пользователей и администраторов. Операции управления жизненным циклом теневых копий (создание, удаление, изменение хранилища) доступны только учетным записям с правами локального администратора. Это является критически важной встроенной мерой защиты от несанкционированного удаления точек восстановления. Стандартные настройки Windows регистрируют в журнале событий только основные системные события VSS (запуск службы, ошибки). Для обеспечения подотчетности (accountability) и возможности расследования инцидентов, связанных с манипуляцией теневых копий, требуется дополнительная ручная настройка расширенных политик аудита объекта (Audit Other Object Access Events). Механизм восстановления данных через «Предыдущие версии» делегирован конечным пользователям и требует от них только стандартных прав на чтение файлов, что соответствует лучшим практикам безопасности.
3. **Практическая оценка защищенности от типовых угроз.** Настроенная конфигурация VSS обеспечивает эффективную защиту от сценария, при котором злоумышленник обладает правами обычного пользователя – удалить теневые копии в этом случае невозможно. Эксперимент выявил ключевой вектор атаки, не устраняемый средствами самой VSS: компрометацию учетной записи администратора. Это соответствует тактике продвинутых ransomware[3] и подчеркивает критическую важность внешних мер по защите учетных записей с повышенными привилегиями, что выходит за рамки настройки VSS, но должно быть частью общей стратегии безопасности.

Таким образом, практическое исследование показало, что грамотно настроенная служба VSS представляет собой надежный и безопасный инструмент для оперативного восстановления данных. Ее базовая конфигурация обеспечивает защиту от наиболее распространенных рисков, связанных с человеческим фактором, однако для соответствия требованиям современной кибербезопасности необходима дополнительная настройка аудита и строгий контроль административных привилегий.

РАЗДЕЛ 5. ЗАКЛЮЧЕНИЕ

В данной работе было проведено исследование, направленное на практическую настройку, функциональное тестирование и анализ вопросов безопасности службы теневого копирования томов (VSS) на платформе Windows Server в изолированной среде виртуализации.

В ходе исследования был успешно развернут тестовый стенд, проведен критический анализ литературных источников и уязвимостей (CVE), выявивший ключевые риски для VSS: атаки на удаление точек восстановления и эксплуатацию уязвимостей для повышения привилегий (например, CVE-2021-28316). На основе этого анализа были сформулированы и экспериментально проверены меры защиты.

Исходная гипотеза о том, что стандартная конфигурация VSS обеспечивает достаточный уровень надежности и защищенности для оперативного восстановления данных после типовых инцидентов, нашла свое подтверждение. Эксперимент показал, что VSS не только выполняет свою основную функцию, но и обладает продуманной моделью безопасности, защищающей механизм восстановления от несанкционированного вмешательства.

Перспективные направления для дальнейших исследований:

1. Глубокое тестирование устойчивости инфраструктуры VSS в условиях моделирования целевых атак, включая сценарии с компрометацией административных учетных записей.
2. Исследование интеграции VSS с системами мониторинга безопасности (SIEM) [8] для централизованного сбора и анализа событий аудита.
3. Сравнительный анализ производительности VSS под высокой нагрузкой и его влияние на работу ресурсоемких приложений (СУБД, почтовые серверы).
4. Изучение возможности использования защищенных, неизменяемых хранилищ для теневых копий в качестве меры противодействия ransomware.

Проведенное исследование демонстрирует, что VSS является ценным встроенным активом операционной системы Windows Server, а его грамотная настройка с учетом рекомендаций по безопасности позволяет существенно повысить отказоустойчивость ИТ-инфраструктуры и снизить риски, связанные с потерей данных.

Использованные источники:

1. 2023 Data Breach Investigations Report (DBIR) // Verizon Business. – 2023. [Электронный ресурс]. URL: https://cisoclub.ru/dbir-kompanii-verizon-vyjavila-34-nyj-rost-chisla-sluchaev-jekspluatacii-ujazvimostej/ (дата обращения: 22.11.2024).
2. Acronis Cyber Protect VSS Troubleshooting Guide [Электронный ресурс] // Acronis Knowledge Base. [Электронный ресурс]. URL: https://care.acronis.com/s/article/Acronis-Cyber-Protect-VSS-Troubleshooting-Guide?language=ru (дата обращения: 15.11.2024).
3. Common TTPs of modern ransomware // Kaspersky. – 2023. [Электронный ресурс]. URL: https://go.kaspersky.com/rs/802-IJN-

240/images/Report_Common%20TTPs%20of%20modern%20ransomware.pdf (дата обращения: 22.11.2024).

4. The April 2021 Security Update Review // Zero Day Initiative (ZDI). – 2021. [Электронный ресурс]. URL: https://www.zerodayinitiative.com/blog/2021/4/13/the-april-2021-security-update-review (дата обращения: 22.11.2024).
5. Volume Shadow Copy Service // Microsoft Learn. – 2023. [Электронный ресурс]. URL: https://learn.microsoft.com/ru-ru/windows-server/storage/file-server/volume-shadow-copy-service (дата обращения: 22.11.2024).
6. Windows Server 2022. Официальная документация // Microsoft Docs. [Электронный ресурс]. URL: https://docs.microsoft.com/ru-ru/windows-server/ (дата обращения: 15.11.2024).
7. Виртуализация с Oracle VM VirtualBox // Oracle Documentation. [Электронный ресурс]. URL: https://www.virtualbox.org/manual/UserManual.html (дата обращения: 15.11.2024).
8. Мунтян Михаил Михайлович, Сидоркина Ирина Геннадьевна Способ интеграции вспомогательного модуля с SIEM-системами // Вестник ЧГУ. 2024. №4. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/sposob-integratsii-vspomogatelnogo-modulya-s-siem-sistemami (дата обращения: 22.11.2025).
9. Уймин, А. Г. Сетевое и системное администрирование. Демонстрационный экзамен КОД 1.1 : учебно-методическое пособие для СПО / А. Г. Уймин. – 3-е изд., стер. – Санкт-Петербург : Лань, 2022. – 480 с. – ISBN 978-5-8114-9255-8.