Научная статья
УДК 004.056.3
https://doi.org/10.31854/1813-324X-2026-12-1-16-25
EDN:YTOMOZ

CC BY 4.0

Комплексный подход к обеспечению непрерывности бизнес-процессов на основе централизованных систем резервирования данных

Сергей Сергеевич Соколов[1], sokolovss@gumrf.ru
Олег Сергеевич Лаута[1] ✉, laos-82@yandex.ru
Михаил Валерьевич Митрофанов[2], vonafortim@yandex.ru
Александр Сергеевич Куракин[3], nirt@mail.ru
Николай Николаевич Крамской[3], kram.com@mail.ru

[1]Государственный университет морского и речного флота им. адмирала С.О. Макарова,
Санкт-Петербург, 198035, Российская Федерация
[2]Национальный исследовательский университет ИТМО,
Санкт-Петербург, 197101, Российская Федерация
[3]ООО «Специальный Технологический Центр»,
Санкт-Петербург, 195220, Российская Федерация

Аннотация

Актуальность. *Современные бизнес-процессы критически зависят от непрерывной доступности данных, при этом частота инцидентов утраты информации из-за ransomware-атак, отказов оборудования и ошибок администраторов устойчиво растет.*
Целью *исследования является разработка и обоснование комплексного подхода к построению централизованных систем резервирования данных, обеспечивающих минимизацию времени восстановления и максимизацию вероятности успешного восстановления при катастрофических сбоях различной природы.*
Методы. *Методологической основой работы выступают системный подход к проектированию архитектуры резервного копирования, методы количественного анализа рисков и сравнительный анализ.*
Решение (результаты). *Разработан комплексный архитектурный подход, основанный на централизованной pull-ориентированной системе резервного копирования. Сформирована методика выбора между полным резервированием дисков и гранулярным файловым резервированием.*
Научная новизна *состоит в обосновании комплексной централизованной системы резервирования данных, объединяющей snapshot-ориентированное резервирование, многоуровневую архитектуру хранения и pull-модель с физически и логически изолированным сервером.*
Теоретическая значимость *заключается в развитии научно-методического аппарата обеспечения непрерывности бизнес-процессов за счет формализации критериев выбора режимов резервирования и архитектурных решений с учетом ограниченности ресурсов и неоднородности данных.*
Практическая значимость *работы проявляется в разработке конкретных архитектурных требований и рекомендаций по построению систем резервного копирования.*

Ключевые слова: *snapshot-технологии, ransomware-атаки, система резервирования данных, защищенность от целенаправленного удаления резервных копий*

Ссылка для цитирования: Соколов С.С., Лаута О.С., Митрофанов М.В., Куракин А.С., Крамской Н.Н. Комплексный подход к обеспечению непрерывности бизнес-процессов на основе централизованных систем резервирования данных // Труды учебных заведений связи. 2026. Т. 12. № 1. С. 16–25. DOI:10.31854/1813-324X-2026-12-1-16-25. EDN:YTOMOZ

© Соколов С.С., Лаута О.С., Митрофанов М.В., Куракин А.С., Крамской Н.Н., 2026

Original research
https://doi.org/10.31854/1813-324X-2026-12-1-16-25
EDN:YTOMOZ

A Comprehensive Approach to Ensuring Business Continuity Based on Centralized Data Backup Systems

Sergey S. Sokolov[1], sokolovss@gumrf.ru
Oleg S. Lauta[1] ✉, laos-82@yandex.ru
Mikhail V. Mitrofanov[2], vonafortim@yandex.ru
Aleksandr S. Kurakin[3], nirt@mail.ru
Nikolay N. Kramskoy[3], kram.com@mail.ru

[1]Admiral Makarov State University of Maritime and Inland Shipping,
St. Petersburg, 198035, Russian Federation
[2]ITMO University,
St. Petersburg, 197101, Russian Federation
[3]Special Technology Center LLC,
Saint Petersburg, 195220, Russian Federation

Annotation

Relevance*. Modern business processes critically depend on the continuous availability of data, while the frequency of data loss incidents due to ransomware attacks, equipment failures, and administrative errors is steadily increasing.*
The purpose of the study *is to develop and validate a comprehensive approach to building centralized data backup systems that minimize recovery time and maximize the likelihood of successful recovery from catastrophic failures of various types.*
Methods*. The methodological basis of this study is a systems approach to backup architecture design, quantitative risk analysis methods, and comparative analysis.*
Solution (Results). *A comprehensive architectural approach based on a centralized pull-oriented backup system has been developed. A methodology for choosing between full disk backup and granular file backup has been formulated.*
The scientific novelty *lies in the justification of a comprehensive centralized data backup system that combines snapshot-oriented backup, a multi-tiered storage architecture, and a pull model with a physically and logically isolated server.*
The theoretical significance *lies in the development of a scientific and methodological framework for ensuring business process continuity by formalizing criteria for selecting backup modes and architectural solutions, taking into account resource limitations and data heterogeneity.*
The practical significance *of the work lies in the development of specific architectural requirements and recommendations for building backup systems.*

Keywords: *snapshot technologies, ransomware attacks, data backup system, protection against targeted deletion of backups*

For citation: Sokolov S.S., Lauta O.S., Mitrofanov M.V., Kurakin A.S., Kramskoy N.N. A Comprehensive Approach to Ensuring Business Continuity Based on Centralized Data Backup Systems. *Proceedings of Telecommunication Universities.* 2026;12(1):16–25. (in Russ.) DOI:10.31854/1813-324X-2026-12-1-16-25. EDN:YTOMOZ

Введение

Современная цифровая экономика характеризуется критической зависимостью бизнес-процессов от непрерывной доступности данных, что делает проблему обеспечения их сохранности одной из центральных в области информационной безопасности предприятий. Анализ инцидентов информационной безопасности за 2024 г. показывает устойчивый рост числа случаев утраты данных вследствие ransomware-атак (увеличение на 15 %), отказов оборудования (25 % всех инцидентов) и ошибок администраторов (35 % случаев). При этом потенциальные финансовые потери от полной утраты данных могут достигать сотен миллионов рублей, а время простоя критически важных сервисов напрямую влияет на конкурентоспособность организации. Практика показывает, что даже крупные дата-центры подвержены катастрофическим рискам: пожары, наводнения, землетрясения и целенаправленные кибератаки способны за считанные минуты уничтожить результаты многолетней работы. В этих условиях резервное копирование данных перестает быть вспомогательной функцией IT-инфраструктуры и становится стратегическим элементом обеспечения непрерывности бизнеса[1,2] [1–3].

Вместе с тем, несмотря на очевидность проблемы, практическая реализация систем резервирования в большинстве организаций характеризуется существенными недостатками, создающими иллюзию защищенности при фактической уязвимости. Слишком многие организации преступно пренебрегают резервным копированием, руководствуясь ошибочными концепциями и техниками, такими как «бэкапы Шрёдингера» – никогда не тестируемые резервные копии, валидность которых остается неизвестной до момента критической необходимости их использования. Распространенным заблуждением является отождествление RAID-массивов с системой резервного копирования, хотя RAID обеспечивает лишь отказоустойчивость на уровне аппаратуры, но не защищает от логических ошибок, вирусных атак или физического уничтожения оборудования. Многие организации полностью полагаются на облачные сервисы, не осознавая, что крупные поставщики облачных услуг работают по модели коллективной ответственности, при которой конечная ответственность за защиту и резервное копирование данных лежит на пользователях, а не на провайдере инфраструктуры. Особенно критичной ошибкой является практика простого копирования файлов работающих баз данных без выполнения надлежащего дампа, что приводит к созданию невосстанавливаемых резервных копий из-за нарушения целостности данных в процессе их изменения. Хранение резервных копий на той же физической машине или в том же сегменте сети, что и основные данные, создает единую точку отказа и делает систему резервирования бесполезной при катастрофических сбоях[1,3] [4–6].

Анализ научно-методического аппарата в области обеспечения непрерывности бизнес-процессов выявляет противоречие между теоретическими подходами к построению систем резервирования и практическими требованиями современных организаций. Существующие методики фокусируются преимущественно на технологических аспектах создания резервных копий, недостаточно учитывая системный характер задачи обеспечения непрерывности бизнеса. В работах, посвященных аварийному восстановлению, основное внимание уделяется таким показателям, как целевое время восстановления (RTO*, аббр. от англ.* Recovery Time Objective) и целевая точка восстановления (RPO, *аббр. от англ.* Recovery Point Objective). Однако методология их оптимизации в условиях ограниченных ресурсов остается недостаточно разработанной. Традиционные подходы рассматривают выбор между резервированием всего диска и отдельных файлов как дихотомию, не предлагая комплексных гибридных решений, адаптированных к специфике различных типов данных и бизнес-процессов. Существует разрыв между теоретическими моделями, предполагающими неограниченные ресурсы хранения и пропускную способность каналов связи, и реальными условиями функционирования организаций, где необходим баланс между безопасностью, стоимостью и скоростью восстановления. Архитектурные решения[1,2,3,4, 5, 6] на основе push-модели (клиент инициирует резервное копирование) и pull-модели (сервер подключается к клиенту) инициации резервного копирования обсуждаются

[1] Маринелли С. Своя система бэкапов: сначала стратегия, потом скрипты // Habr. URL: https://habr.com/ru/companies/ruvds/articles/929830/ (дата обращения 28.12.2025)

[2] Impact of Backup Technology on Business Continuity // Unisense Advisory. URL: https://unisenseadvisory.com/impact-of-backup-technology-on-business-continuity [Accessed 28.12.2025]

[3] Offsite Data Backup Storage And Disaster Recovery Guide // Zmanda. URL: https://www.zmanda.com/blog/offsite-data-backup-storage-and-disaster-recovery [Accessed 28.12.2025]

[4] IT Disaster Recovery Methodology and Guidelines // Bryant University. URL: https://is.bryant.edu/about/policies/it-disaster-recovery-methodology-and-guidelines [Accessed 28.12.2025]

[5] RPO and RTO impact on sizing // Exasol Documentation. URL: https://docs.exasol.com/db/latest/planning/business_continuity/impact_rpo_rto.htm [Accessed 28.12.2025]

[6] What's your RTO/RPO and how do you calculate it? // N-able Blog. URL: https://www.n-able.com/es/blog/whats-your-rtorpo-and-how-do-you-calculate-it [Accessed 28.12.2025]

изолированно от вопросов информационной безопасности, не учитывая риски компрометации серверов резервного копирования при атаках на клиентские системы [7–9].

Настоящее исследование основывается на гипотезе, что комплексная централизованная система резервирования данных, интегрирующая технологии snapshot-based копирования, многоуровневую архитектуру хранения и автоматизированные механизмы верификации, способна обеспечить качественно новый уровень непрерывности бизнес-процессов при приемлемых экономических затратах.

Предполагается, что использование нативных возможностей файловых систем с поддержкой снэпшотов (ZFS, BTRFS) в сочетании с централизованным pull-based сервером резервирования позволит достичь значений RTO менее 1 часа и RPO – менее 15 минут даже для критически важных систем объемом несколько терабайт. Гипотеза включает предположение о том, что архитектура с физической и логической изоляцией сервера резервного копирования, дополненная собственными снэпшотами на стороне сервера, обеспечит защиту от наиболее опасного сценария – целенаправленного удаления резервных копий после компрометации производственных систем. Ожидается, что экономический эффект от снижения рисков утраты данных и сокращения времени простоя превысит дополнительные затраты на реализацию предлагаемой системы в течение трех лет эксплуатации (https://habr.com/ru/companies/ruvds/articles/929830, https://unisenseadvisory.com/impact-of-backup-technology-on-business-continuity, https://www.zmanda.com/blog/offsite-data-backup-storage-and-disaster-recovery, https://docs.exasol.com/db/latest/planning/business_continuity/impact_rpo_rto.htm).

Целью настоящего исследования является разработка и обоснование комплексного подхода к построению централизованных систем резервирования данных, обеспечивающих минимизацию времени восстановления и максимизацию вероятности успешного восстановления при катастрофических сбоях различной природы.

Для достижения поставленной цели необходимо решить следующие задачи:

– провести систематический анализ рисков утраты данных в современных IT-инфраструктурах и количественно оценить потенциальные финансовые последствия различных сценариев инцидентов;

– разработать архитектуру централизованной системы резервирования, оптимизирующую соотношение между показателями безопасности (физическая удаленность хранения), доступности (скорость восстановления) и экономической эффективности (стоимость хранения и каналов передачи данных);

– формализовать методику выбора между полным резервированием дисков и гранулярным резервированием файлов с учетом типа данных, критичности систем и технологических возможностей платформы виртуализации;

– разработать математическую модель оценки показателей RTO и RPO в зависимости от параметров системы резервирования (частота создания резервных копий, объем данных, пропускная способность канала, наличие локальных снэпшотов);

– провести сравнительный анализ эффективности традиционных и предлагаемого подхода на основе количественных показателей времени восстановления, допустимой потери данных и вероятности успешного восстановления.

Комплексный подход выбора между полным резервированием дисков и гранулярным резервированием файлов с учетом типа данных

Методология исследования базируется на системном подходе к проектированию архитектуры резервного копирования, начиная с формулирования стратегических вопросов, определяющих требования к системе. Первичным этапом является оценка приемлемого уровня риска для организации, что требует ответа на фундаментальные вопросы: какой риск является приемлемым, какие данные требуют защиты, с каким временем простоя организация готова мириться, и какой объем ресурсов хранения доступен для реализации системы резервирования. На основе этих параметров формируется политика резервного копирования, обеспечивающая баланс между безопасностью и стоимостью реализации.

Ключевым принципом разрабатываемого комплексного подхода является признание того, что самый безопасный бэкап – это тот, который хранится максимально удаленно от исходной машины, однако при этом возникают ограничения, связанные с шириной канала передачи данных и временем восстановления.

При проектировании системы необходимо учитывать, что безопасность не всегда равна практичности: при скорости передачи 200 Мбит/с восстановление 2 ТБ данных потребует существенного времени, что может быть неприемлемо для критически важных сервисов [10].

Комплексный подход предусматривает решение о выборе между резервированием всего диска или отдельных файлов на основе анализа преимуществ и недостатков каждого подхода. Резервирование всего диска обеспечивает полное восстановление системы, включая загрузчик, эффективную интеграцию с системами виртуализации и возможность быстрого клонирования виртуальных машин, однако требует остановки физических серверов для создания консистентной копии и значительных

объемов хранения. Резервирование отдельных файлов позволяет использовать стандартные утилиты, выполнять дельта-копирование только измененных частей, применять сжатие и дедупликацию, а также осуществлять резервное копирование без остановки систем, но создает риски несогласованности данных при копировании «живых» файловых систем (https://habr.com/ru/companies/ruvds/articles/929830, https://docs.exasol.com/db/latest/planning/business_continuity/impact_rpo_rto.htm).

Критически важным элементом является решение проблемы согласованности данных при резервном копировании работающих систем. Резервное копирование «живой» файловой системы характеризуется наличием моментов начала и завершения процесса, между которыми данные могут изменяться, что приводит к фатальным несоответствиям и невозможности восстановления, особенно для файлов баз данных. Решением этой проблемы является обязательное создание снэпшота файловой системы перед началом резервного копирования, что обеспечивает замороженный согласованный слепок данных на определенный момент времени.

Комплексный подход предусматривает использование различных механизмов создания снэпшотов в зависимости от используемой платформы:

– нативные снэпшоты файловых систем с встроенной поддержкой (ZFS, BTRFS);

– снэпшоты *LVM* для пользователей систем логического управления томами;

– специализированные инструменты типа DattoBD для сред без нативной поддержки снэпшотов.

Архитектурное решение предполагает выбор между push-моделью (клиент инициирует резервное копирование) и pull-моделью (сервер подключается к клиенту). Разрабатываемая методика отдает предпочтение централизованным системам на базе выделенных серверов резервного копирования, работающих в окружениях с высокой степенью безопасности и минимальным количеством сервисов, что соответствует pull-архитектуре. При этом критически важно, чтобы сервер резервного копирования не был доступен извне и мог взаимодействовать только с системами, резервное копирование которых он выполняет, минимизируя вероятность компрометации или удаления резервных копий при атаке на клиентские машины. Дополнительным уровнем защиты является хранение собственных снэпшотов файловой системы на сервере резервного копирования, недоступных со стороны клиентов, что обеспечивает возможность восстановления даже при сценарии целенаправленного удаления резервных копий после компрометации производственных систем (https://habr.com/ru/companies/ruvds/articles/929830, https://docs.exasol.com/db/latest/planning/business_continuity/impact_rpo_rto.htm).

Комплексный подход формулирует ключевые требования к качественной системе резервного копирования. Система должна обеспечивать мгновенное восстановление и работать с высокой скоростью, минимизируя время простоя бизнес-сервисов. Обязательным требованием является внешнее хранение резервных копий вне системы, резервирование которой выполняется, при одновременном создании локальных снэпшотов для быстрых откатов при незначительных инцидентах. Базовое требование – самостоятельное управление критически важными данными без полной зависимости от публичных облачных сервисов, что обеспечивает контроль над процессом резервирования и восстановления. Эффективное управление пространством хранения достигается за счет использования механизмов сжатия и дедупликации на уровне файловой системы или блочных устройств. Минимальная инвазивность системы предполагает, что для ее работы требуется минимальное количество дополнительных компонентов на клиентских машинах, что упрощает администрирование и снижает риски конфликтов.

Математическая модель, связывающая ключевые параметры системы с показателями непрерывности бизнеса

Для количественной оценки эффективности различных подходов к резервированию данных разработана математическая модель, связывающая ключевые параметры системы с показателями непрерывности бизнеса. Целевое время восстановления RTO определяется совокупностью факторов, включающих объем восстанавливаемых данных V, пропускную способность канала передачи B, эффективность алгоритмов сжатия и дедупликации k_c, а также время, необходимое на подготовительные операции t_p [11].

Упрощенная модель времени восстановления имеет вид:

$$\mathrm{RTO} = V/(B \cdot k_c) + t_p, \quad (1)$$

где коэффициент сжатия k_c для современных систем с дедупликацией может достигать значений 2–5 в зависимости от типа данных.

Целевая точка восстановления RPO определяется частотой создания резервных копий f и временем хранения входных транзакций, при этом максимальный возраст резервной копии вычисляется по выражению:

$$\mathrm{RPO}_{\max} = t_{\mathrm{storage}} - t_{\mathrm{restore}}, \quad (2)$$

где t_{storage} – время хранения входных данных; t_{restore} – время восстановления резервной копии.

Для критически важных систем с требованием RPO менее 1 часа необходима реализация непрерывной защиты данных (CDP) или создание снэпшотов с интервалом 15–30 минут (https://docs.exasol.com/db/latest/planning/business_continuity/impact_rpo_rto.htm).

Сравнительный анализ различных подходов к организации резервного копирования

Сравнительный анализ различных подходов к организации резервного копирования проведен на основе количественных показателей эффективности. Рассмотрены четыре варианта реализации: локальное копирование на внешние накопители, использование облачного хранилища, традиционная централизованная система и предлагаемый комплексный подход с интеграцией snapshot-технологий.

Анализ показывает, что локальное копирование характеризуется наихудшими показателями RTO и RPO (24 часа для обоих параметров), минимальной стоимостью реализации (5000 условных единиц), низкой сложностью администрирования, но критически низкой вероятностью успешного восстановления (65 %) вследствие рисков физического повреждения носителей и отсутствия географической избыточности. Облачное хранилище обеспечивает улучшенные показатели RTO = 12 часов и RPO = 6 часов, повышенную вероятность восстановления (75 %), но требует существенных периодических затрат (15000 условных единиц) и создает зависимость от внешнего провайдера. Традиционная централизованная система демонстрирует значительное улучшение временны́х характеристик (RTO = 2 часа, RPO = 1 час) и высокую вероятность успешного восстановления (95 %), однако отличается повышенной сложностью администрирования [12].

Предлагаемый комплексный подход обеспечивает качественно новые показатели:

– RTO = 0,5 часа;

– RPO = 0,25 часа (15 минут);

– вероятность успешного восстановления составляет 98 % при умеренной сложности администрирования благодаря автоматизации процессов.

Количественная оценка рисков различных сценариев утраты данных позволяет рассчитать экономическую эффективность внедрения предлагаемой системы.

Анализ охватывает основные категории инцидентов с различной вероятностью возникновения и потенциальным ущербом:

– пожар в дата-центре, имеющий вероятность 0,5 % в год, способен привести к потерям 150 млн рублей при отсутствии резервирования, 50 млн при традиционном подходе и лишь 5 млн рублей при использовании предлагаемой системы;

– ransomware-атаки, вероятность которых составляет 15 % и продолжает расти, приводят к потерям 80 млн рублей без защиты, 40 млн при традиционном резервировании и всего 2 млн рублей при предлагаемом подходе благодаря изолированному хранению снэпшотов;

– отказ оборудования как наиболее частый инцидент (вероятность 25 %) влечет потери 25, 10 и 0,5 млн рублей соответственно для следующих рассматриваемых сценариев:

1) ошибки администраторов с максимальной вероятностью 35 % приводят к сравнительно небольшим потерям (10 млн рублей без защиты, 5 млн при традиционном подходе, 0,1 млн рублей при предлагаемом решении) благодаря возможности быстрого восстановления из локальных снэпшотов;

2) стихийные бедствия при низкой вероятности (1 %) характеризуются катастрофическим потенциальным ущербом до 200 млн рублей, который снижается до 80 и 10 млн соответственно (https://habr.com/ru/companies/ruvds/articles/929830);

Расчет математического ожидания потерь показывает, что традиционный подход характеризуется ожидаемым ущербом 11,3 млн рублей в год, тогда как предлагаемая система снижает этот показатель до 0,58 млн, обеспечивая экономический эффект 10,71 млн рублей ежегодно. При стоимости реализации предлагаемой системы 30000 условных единиц срок окупаемости инвестиций составляет 2,8 г., что является приемлемым для систем обеспечения непрерывности бизнеса. Особенно значимым результатом является снижение потерь от ransomware-атак – с 6 до 0,3 млн рублей в год (ожидаемое значение с учетом вероятности), что в условиях роста киберугроз представляет критически важное преимущество.

Анализ зависимости времени восстановления от объема резервируемых данных демонстрирует устойчивое преимущество предлагаемого подхода во всем диапазоне объемов (рисунок 1). Для объема данных в 100 Гб традиционный подход требует 1,2 часа на восстановление, тогда как предлагаемая система сокращает это время до 0,2 часа, обеспечивая выигрыш 83,3 %. При увеличении объема до 500 Гб время восстановления составляет 6 и 1 час соответственно, при 1000 Гб – 12 и 2 часа, при 2000 Гб – 24 и 4 часа. Даже для больших объемов данных (5000 ГБ) предлагаемая система обеспечивает восстановление за 10 часов вместо 60 часов при традиционном подходе, сохраняя относительное преимущество на уровне 83 %. Такое улучшение достигается за счет комбинации факторов: использования высокоскоростных каналов связи между сервером резервирования и клиентскими системами, эффективной дедупликации и сжатия

на уровне файловой системы ZFS, возможности параллельного восстановления из нескольких снэпшотов и оптимизированных алгоритмов передачи только измененных блоков данных https://habr.com/ru/companies/ruvds/articles/929830.

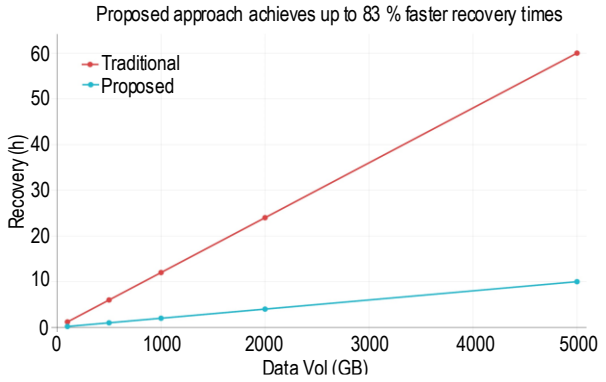

Рис. 1. Зависимость времени восстановления данных от объема резервируемой информации

Fig. 1. Dependence of Data Recovery Time on the Volume of Backed-Up Information

Графическое представление сравнительного анализа целевых показателей восстановления наглядно демонстрирует качественное превосходство предлагаемого подхода (рисунок 2). Визуализация показывает экспоненциальное снижение как времени восстановления (RTO), так и допустимой потери данных (RPO) при переходе от локального копирования через облачное хранилище и традиционную централизованную систему к предлагаемому комплексному решению. Особенно значимым является достижение субчасовых значений обоих показателей (0,5 часа RTO и 0,25 часа RPO), что переводит систему в категорию решений высокой доступности, приближающихся по характеристикам к системам непрерывной репликации при существенно меньшей стоимости реализации (https://unisenseadvisory.com/impact-of-backup-technology-on-business-continuity).

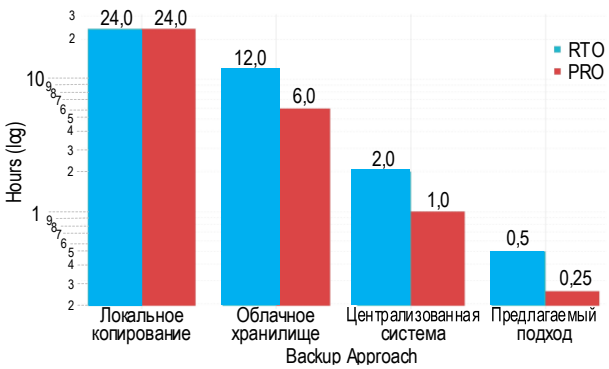

Рис. 2. Сравнительный анализ целевых показателей восстановления (RTO/RPO) для различных подходов к резервированию данных

Fig. 2. Comparative Analysis of Recovery Targets (RTO/RPO) for Different Data Backup Approaches

Результаты исследования демонстрируют, что комплексный подход к построению централизованных систем резервирования данных на основе snapshot-технологий обеспечивает качественное улучшение показателей непрерывности бизнеса при приемлемых экономических затратах. Достигнуто сокращение целевого времени восстановления до 30 минут и целевой точки восстановления до 15 минут, что на 83 % превосходит традиционные подходы к резервированию.

Вероятность успешного восстановления увеличена до 98 % благодаря использованию нативных механизмов снэпшотов файловых систем, обеспечивающих консистентность данных, и многоуровневой архитектуры хранения с физической изоляцией сервера резервного копирования. Экономическая эффективность предлагаемого решения подтверждается снижением математического ожидания потерь с 11,3 до 0,58 млн рублей в год при сроке окупаемости инвестиций менее трех лет. Особенно значимым результатом является повышение устойчивости к ransomware-атакам за счет архитектуры с изолированными снэпшотами на стороне сервера, недоступными для модификации или удаления со стороны скомпрометированных клиентских систем.

В таблице 1 представлено комплексное сравнение различных подходов к резервированию данных по шести ключевым характеристикам:

– локальное копирование (LC);
– облачное хранилище (CloudStorage);
– централизованная система (CSyst);
– предлагаемый подход (ПП).

ТАБЛИЦА 1. Комплексное сравнение различных подходов к резервированию данных

TABLE 1. A Comprehensive Comparison of Various Approaches to Data Backup

Характеристика	LC	Cloud Storage	CSyst	ПП
Время восстановления (RTO), ч	24,0	12,0	2,0	0,50
Допустимая потеря данных (RPO), ч	24,0	6,0	1,0	0,25
Требуемое пространство хранения, ТБ	2,0	1,5	3,0	3,50
Стоимость реализации, у.е.	5000	15000	25000	30000
Сложность администрирования (1–5)	2	3	4	3
Вероятность успешного восстановления, %	65	75	95	98

Предлагаемый подход демонстрирует оптимальное сочетание минимальных значений RTO (0,5 ч) и RPO (0,25 ч) с максимальной вероятностью успешного восстановления (98 %) при умеренной

сложности администрирования, достигаемой благодаря высокой степени автоматизации процессов резервного копирования и восстановления.

Анализ рисковых сценариев, представленный в таблице 2, количественно обосновывает экономическую целесообразность внедрения предлагаемой системы. Совокупный выигрыш по пяти категориям инцидентов составляет от 4,9 млн рублей для наиболее частых ошибок администраторов до 70 млн рублей для катастрофических стихийных бедствий, подтверждая эффективность многоуровневой защиты данных.

ТАБЛИЦА 2. Результаты анализа рисковых сценариев

TABLE 2. Results of Risk Scenario Analysis

Сценарий	P	$L_{без\ резерв}$	$L_{тп}$,	$L_{ппп}$,	G,
Пожар в ЦОД	0,5	150	50	5,0	45,0
Ransomware-атака	15,0	80	40	2,0	38,0
Отказ оборудования	25,0	25	10	0,5	9,5
Ошибка администратора	35,0	10	5	0,1	4,9
Стихийное бедствие	1,0	200	80	10,0	70,0

Усл. обозначения: P – вероятность, %; $L_{без\ резерв}$ – потери без резервирования, млн руб.; $L_{тп}$– потери (традиционный подход), млн руб.; $L_{ппп}$ – потери (предлагаемый подход), млн руб.; G – выигрыш, млн руб.

Заключение

Проведенное исследование позволяет сформулировать ряд практических рекомендаций по построению эффективных систем обеспечения непрерывности бизнес-процессов. Первоочередным требованием является отказ от концепции резервного копирования как вспомогательной функции и признание ее стратегическим элементом информационной безопасности организации, что должно найти отражение в выделении адекватных ресурсов и приоритизации задач. Необходимо начинать проектирование системы резервирования с формулирования политики, основанной на ответах на фундаментальные вопросы о приемлемом уровне риска, критичности различных категорий данных, допустимом времени простоя и доступных ресурсах. Обязательным элементом любой системы резервирования должно быть создание снэпшотов файловых систем перед началом копирования для обеспечения консистентности данных, что требует использования файловых систем с нативной поддержкой снэпшотов (ZFS, BTRFS) или внедрения соответствующих технологий на уровне LVM. Архитектура системы должна предусматривать физическую и логическую изоляцию сервера резервного копирования с ограничением доступа только к необходимым клиентским системам и обязательным созданием собственных снэпшотов, недоступных для модификации со стороны клиентов. Критически важным является регулярное тестирование процедур восстановления, поскольку не тестируемые резервные копии («бэкапы Шредингера») создают лишь иллюзию защищенности без гарантии успешного восстановления в критической ситуации. Организациям следует избегать полной зависимости от публичных облачных сервисов для хранения критически важных данных, сохраняя контроль над процессом резервирования и физическим размещением резервных копий.

Дальнейшее развитие исследований в области обеспечения непрерывности бизнес-процессов должно быть направлено на интеграцию технологий искусственного интеллекта для прогнозирования отказов и оптимизации параметров резервирования в реальном времени. Перспективным направлением является разработка адаптивных систем, автоматически корректирующих частоту создания резервных копий и политики хранения в зависимости от интенсивности изменения данных и текущего уровня угроз. Требуют дополнительного исследования вопросы оптимизации топологии размещения серверов резервного копирования с учетом географических рисков, стоимости каналов связи и нормативных требований к локализации данных. Актуальной задачей остается разработка формализованных методик оценки совокупной стоимости владения системами резервирования с учетом не только прямых затрат на оборудование и каналы связи, но и косвенных эффектов от снижения рисков простоя бизнес-сервисов и репутационных потерь.

Список источников

1. Hou Y., Guo L., Zhou C., Xu Y., Yin Z., Li S., et al. An Empirical Study of Data Disruption by Ransomware Attacks // Proceedings of the 46th International Conference on Software Engineering (ICSE '24, Lisbon, Portugal, 14–20 April 2024). New York: Association for Computing Machinery, 2024. P. 161. DOI:10.1145/3597503.3639090

2. Al-rimy B.A.S., Maarof M.A., Shaid S.Z.M. Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions // Computers & Security. 2018. Vol. 74. PP. 144–166. DOI:10.1016/j.cose.2018.01.001

3. Котенко И.В., Саенко И.Б., Лаута О.С., Васильев Н.А., Садовников В.Е. Метод противодействия состязательным атакам на системы классификации изображений // Вопросы кибербезопасности. 2025. № 2(66). С. 114–123. DOI:10.21681/2311-3456-2025-2-114-123. EDN:MKWZFT

4. Hou Y., Guo L., Zhou C., Zhang Q., Liu W., Sun C., et al. Preventing Disruption of System Backup against Ransomware Attacks // Proceedings of the ACM on Software Engineering. 2025. Vol. 2. Iss. ISSTA. PP. 229–249. DOI:10.1145/3728880. EDN:XZVFZD
5. Zhou C., Guo L., Hou Y., Ma Z., Zhang Q., Wang M. Limits of I/O Based Ransomware Detection: An Imitation Based Attack // Proceedings of the Symposium on Security and Privacy (SP, San Francisco, USA, 21–25 May 2023). IEEE, 2023. DOI:10.1109/SP46215.2023.10179372
6. Kolodenker E., Koch W., Stringhini G., Egele M. PayBreak: Defense Against Cryptographic Ransomware // Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security (ASIACCS, Abu Dhabi, United Arab Emirates, 2–6 April 2017). New York: Association for Computing Machinery, 2017. PP. 599–611. DOI:10.1145/3052973.3053035
7. Николаев В.В., Саенко И.Б. Оптимизация распределения информационных ресурсов в едином информационном пространстве // Труды учебных заведений связи. 2024. Т. 10. № 3. С. 87–103. DOI:10.31854/1813-324X-2024-10-3-87-103. EDN:UFROMW
8. Hirano M., Hodota R., Kobayashi R. RanSAP: An open dataset of ransomware storage access patterns for training machine learning models // Forensic Science International: Digital Investigation. 2021. Vol. 40. P. 301314 DOI:10.1016/j.fsidi.2021.301314. EDN:OZNYCW
9. Hirano M., Kobayashi R. RanSMAP: Open dataset of Ransomware Storage and Memory Access Patterns for creating deep learning based ransomware detectors // Computers & Security. 2025. Vol. 150. P. 104202. DOI:10.1016/j.cose.2024.104202. EDN:GUQFQK
10. Min D., Park Y., Yoon S., Walker R., Lee J., Park S. Amoeba: An Autonomous Backup and Recovery SSD for Ransomware Attack Defense // IEEE Computer Architecture Letters. 2018. Vol. 17. Iss. 2. PP. 245–248. DOI:10.1109/LCA.2018.2883431
11. Ilau M.-C., Baldwin A., Caulfield T., Pym D. Modelling and simulating organizational ransomware recovery: structure, methodology, and decisions // Journal of Cybersecurity. 2025. Vol. 11. Iss. 1. DOI:10.1093/cybsec/tyaf035
12. Kritika Er. A comprehensive literature review on ransomware detection using deep learning techniques // Cyber Security and Applications. 2025. Vol. 3. P. 100078. DOI:10.1016/j.csa.2024.100078

References

1. Hou Y., Guo L., Zhou C., Xu Y., Yin Z., Li S., et al. An Empirical Study of Data Disruption by Ransomware Attacks. *Proceedings of the 46th International Conference on Software Engineering, ICSE '24, 14–20 April 2024, Lisbon, Portugal*. New York: Association for Computing Machinery; 2024. p.161. DOI:10.1145/3597503.3639090
2. Al-rimy B.A.S., Maarof M.A., Shaid S.Z.M. Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. *Computers & Security*. 2018;74:144–166. DOI:10.1016/j.cose.2018.01.001
3. Kotenko I.V., Saenko I.B., Lauta O.S., Vasiliev N.A., Sadovnikov V.E. A Method of countering adversarial attacks on image classification systems. *Cybersecurity Issues*. 2025;2(66):114–123. (in Russ.) DOI:10.21681/2311-3456-2025-2-114-123. EDN:MKWZFT
4. Hou Y., Guo L., Zhou C., Zhang Q., Liu W., Sun C., et al. Preventing Disruption of System Backup against Ransomware Attacks. *Proceedings of the ACM on Software Engineering*. 2025;2(ISSTA):229–249. DOI:10.1145/3728880. EDN:XZVFZD
5. Zhou C., Guo L., Hou Y., Ma Z., Zhang Q., Wang M. Limits of I/O Based Ransomware Detection: An Imitation Based Attack. *Proceedings of the Symposium on Security and Privacy, SP, 21–25 May 2023, San Francisco, USA*. IEEE; 2023. DOI:10.1109/SP46215.2023.10179372
6. Kolodenker E., Koch W., Stringhini G., Egele M. PayBreak: Defense Against Cryptographic Ransomware. *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, ASIACCS, 2–6 April 2017, Abu Dhabi, United Arab Emirates*. New York: Association for Computing Machinery; 2017. p.599–611. DOI:10.1145/3052973.3053035
7. Nikolaev V.V., Saenko I.B. Optimization of Information Resources Distribution in Common Information Space. *Proceedings of Telecommunication Universities*. 2024;10(3):87–103. (in Russ.) DOI:10.31854/1813-324X-2024-10-3-87-103. EDN:UFROMW
8. Hirano M., Hodota R., Kobayashi R. RanSAP: An open dataset of ransomware storage access patterns for training machine learning models. *Forensic Science International: Digital Investigation*. 2021;40:301314 DOI:10.1016/j.fsidi.2021.301314. EDN:OZNYCW
9. Hirano M., Kobayashi R. RanSMAP: Open dataset of Ransomware Storage and Memory Access Patterns for creating deep learning based ransomware detectors. *Computers & Security*. 2025;150:104202. DOI:10.1016/j.cose.2024.104202. EDN:GUQFQK
10. Min D., Park Y., Yoon S., Walker R., Lee J., Park S. Amoeba: An Autonomous Backup and Recovery SSD for Ransomware Attack Defense. *IEEE Computer Architecture Letters*. 2018;17(2):245–248. DOI:10.1109/LCA.2018.2883431
11. Ilau M.-C., Baldwin A., Caulfield T., Pym D. Modelling and simulating organizational ransomware recovery: structure, methodology, and decisions // Journal of Cybersecurity. 2025;11(1). DOI:10.1093/cybsec/tyaf035
12. Kritika Er. A comprehensive literature review on ransomware detection using deep learning techniques. *Cyber Security and Applications*. 2025;3:100078. DOI:10.1016/j.csa.2024.100078

Статья поступила в редакцию 12.12.2025; одобрена после рецензирования 10.02.2026; принята к публикации 16.02.2026.
The article was submitted 12.12.2025; approved after reviewing 10.02.2026; accepted for publication 16.02.2026.

Информация об авторах:

СОКОЛОВ Сергей Сергеевич
доктор технических наук, профессор, ректор Государственного университета морского и речного флота им. адмирала С.О. Макарова
https://orcid.org/0000-0002-4581-2518

ЛАУТА Олег Сергеевич
доктор технических наук, доцент, профессор кафедры «Комплексного обеспечения информационной безопасности» Государственного университета морского и речного флота им. адмирала С.О. Макарова
https://orcid.org/0000-0001-7826-9083

МИТРОФАНОВ Михаил Валерьевич
доктор технических наук, доцент, доцент Военного учебного центра Национального исследовательского университета ИТМО
https://orcid.org/0000-0002-4080-4340

КУРАКИН Александр Сергеевич
кандидат технических наук, начальник направления ООО «Специальный Технологический Центр»
https://orcid.org/0000-0001-7199-6384

КРАМСКОЙ Николай Николаевич
заместитель директора по разработке специальных средств – генеральный конструктор систем и комплексов криптографической защиты информации ООО «Специальный Технологический Центр»
https://orcid.org/0009-0005-2352-985X

Авторы сообщают об отсутствии конфликтов интересов.
The authors declare no conflicts of interests.