А. А. Семенков

УПРАВЛЕНИЕ РЕЗЕРВНЫМ КОПИРОВАНИЕМ, АВАРИЙНЫМ ВОССТАНОВЛЕНИЕМ И ПАРАМЕТРАМИ RPO/RTO В SAP-ИНФРАСТРУКТУРЕ НА БАЗЕ SAP HANA И Oracle

Методическое пособие

А. А. Семенков

УПРАВЛЕНИЕ РЕЗЕРВНЫМ КОПИРОВАНИЕМ, АВАРИЙНЫМ ВОССТАНОВЛЕНИЕМ И ПАРАМЕТРАМИ *RPO/RTO* В *SAP*-ИНФРАСТРУКТУРЕ НА БАЗЕ *SAP HANA* И *Oracle*

Методическое пособие

Белгород 2026

ББК 46я73
С 28

Автор-составитель
А. А. Семенков – ведущий консультант, IBS (г. Ульяновск)

Семенков А. А.

С 28 Управление резервным копированием, аварийным восстановлением и параметрами RPO/RTO в SAP-инфраструктуре на базе SAP HANA и Oracle : методическое пособие / А. А. Семенков. – Белгород : ООО «Эпицентр», 2026. – 38 с.

ISBN 978-5-6056450-7-8

Методическое пособие посвящено систематизации подходов к управлению резервным копированием, аварийным восстановлением и контролю ключевых показателей RPO (Recovery Point Objective) и RTO (Recovery Time Objective) в корпоративных системах на базе SAP HANA и Oracle. Актуальность темы обусловлена ростом зависимости бизнеса от непрерывной работы ERP-систем: по данным Gartner, средняя стоимость одного часа простоя критической информационной системы превышает 300 000 долларов США. Целью работы является разработка методической базы для проектирования стратегий резервного копирования, расчёта ёмкости хранилища и планирования процедур аварийного восстановления с соблюдением целевых значений RPO и RTO. В работе применяются методы системного анализа, математического моделирования темпов роста данных и сравнительного анализа технологий защиты данных. Результатом является комплексная методика, охватывающая все этапы жизненного цикла резервной копии в SAP-инфраструктуре. Сведения, отраженные в рамках пособия, будут представлять интерес специалистам по администрированию баз данных, архитекторам SAP-систем, а также преподавателям и студентам профильных IT-специальностей.

ББК 46я73

ISBN 978-5-6056450-7-8

СОДЕРЖАНИЕ

Введение

Непрерывность функционирования корпоративных информационных систем является одним из ключевых требований современного бизнеса. Системы планирования ресурсов предприятия (ERP) класса SAP обеспечивают поддержку критически важных бизнес-процессов: финансового учёта, управления цепочками поставок, производственного планирования и управления персоналом. Любой сбой в работе такой системы влечёт прямые и косвенные потери, масштаб которых может достигать нескольких миллионов долларов в сутки [1].

По данным исследования IDC за 2024 год, 80% организаций, потерявших доступ к корпоративным данным на срок свыше 72 часов, прекращают деятельность в течение трёх лет [2]. Одновременно аналитики Gartner фиксируют, что лишь 43% предприятий располагают задокументированным и протестированным планом аварийного восстановления, включающим конкретные целевые значения RPO и RTO [3]. Данный разрыв между декларируемыми намерениями и реальной готовностью к восстановлению систем формирует актуальный научный и практический запрос на систематизированные методические рекомендации.

Научный пробел в данной области обусловлен фрагментарностью существующей литературы: большинство публикаций либо описывают архитектурные возможности конкретных платформ (SAP HANA System Replication, Oracle Data Guard), либо фокусируются на общих принципах управления непрерывностью бизнеса (ISO 22301) без детального рассмотрения инженерных методик расчёта параметров резервной инфраструктуры [4, 5].

Целью работы является формирование основы для проектирования, реализации и верификации стратегии резервного копирования и аварийного восстановления SAP-систем на базе HANA и Oracle с соблюдением целевых показателей RPO и RTO.

Научная новизна состоит в интеграции инженерных методик расчёта ёмкости хранилища с процессным подходом к управлению жизненным циклом резервных копий применительно к гибридным SAP-инфраструктурам на базе SAP HANA и Oracle.

Авторская гипотеза: применение многоуровневой модели резервного копирования, сочетающей полные, инкрементальные, дифференциальные и журнальные копии с чётко заданными интервалами, позволяет достигнуть целевых значений RPO менее 15 минут и RTO менее 60 минут без пропорционального увеличения затрат на инфраструктуру хранения.

Раздел 1. Концептуальные основы защиты данных в корпоративных SAP-системах

1.1. Непрерывность бизнеса и защита данных как приоритет эксплуатации ERP

Концепция непрерывности бизнеса (Business Continuity Management, BCM) формирует организационно-технический базис для противодействия угрозам прерывания деятельности предприятия. Применительно к ERP-системам она материализуется прежде всего в требованиях к доступности, целостности и восстанавливаемости данных. SAP-инфраструктура занимает в этой системе приоритетное место: именно в базах данных SAP HANA и Oracle сосредоточены транзакционные данные, регистры финансовой отчётности и операционные показатели, без которых компания не способна функционировать даже в течение нескольких часов [6].

Стандарт ISO 22301:2019 определяет BCM как целостную управленческую систему, в которой технические меры защиты данных выступают одним из уровней обеспечения операционной устойчивости. Согласно модели этого стандарта, резервное копирование и аварийное восстановление относятся к классу защитных мер уровня информационных технологий [7]. Однако задача специалиста SAP-инфраструктуры состоит не только в выполнении копий по расписанию, но и в обеспечении соответствия сформированной системы требованиям бизнеса, выраженным через показатели RPO и RTO.

В контексте корпоративных SAP-систем на базе SAP HANA защита данных приобретает значение по нескольким причинам. Во-первых, SAP HANA является in-memory СУБД, где вся оперативная работа с данными происходит в оперативной памяти. Потеря питания или аппаратный сбой без адекватной защиты на уровне персистентности влечёт полную утрату незафиксированных транзакций [8]. Во-вторых, архитектура SAP-ландшафта, как правило, включает несколько взаимосвязанных систем (ERP, CRM, BW/4HANA, Solution Manager), что делает частичное восстановление технически сложной задачей и повышает

требования к согласованности точек восстановления. В-третьих, регуляторные требования, в частности GDPR и стандарты финансовой отчётности, предписывают сохранность и доступность определённых категорий данных в течение установленных периодов, что должно учитываться при проектировании политик хранения резервных копий [9].

Таким образом, управление резервным копированием в SAP-инфраструктуре следует рассматривать как интегральную дисциплину, объединяющую организационную политику BCM, технические возможности платформ SAP HANA и Oracle и экономически обоснованные решения по архитектуре хранилища.

Переходя от концептуального уровня к операционному, необходимо рассмотреть метрики, через которые требования к защите данных выражаются в измеримых инженерных параметрах.

1.2. Показатели RPO и RTO в системе требований к SAP-инфраструктуре

Recovery Point Objective (RPO) и Recovery Time Objective (RTO) являются операционными метриками, определяющими допустимые границы потерь данных и простоя системы соответственно. RPO задаёт максимально приемлемый период, за который могут быть утрачены данные при аварии: иными словами, это расстояние во времени от момента сбоя до последней успешно сохранённой точки восстановления. RTO определяет, в течение какого времени система должна быть восстановлена и готова к эксплуатации после наступления аварийного события [10].

Ниже представлена схема, иллюстрирующая соотношение RPO и RTO на временной шкале аварийного события и их связь с технологическими решениями по защите данных.

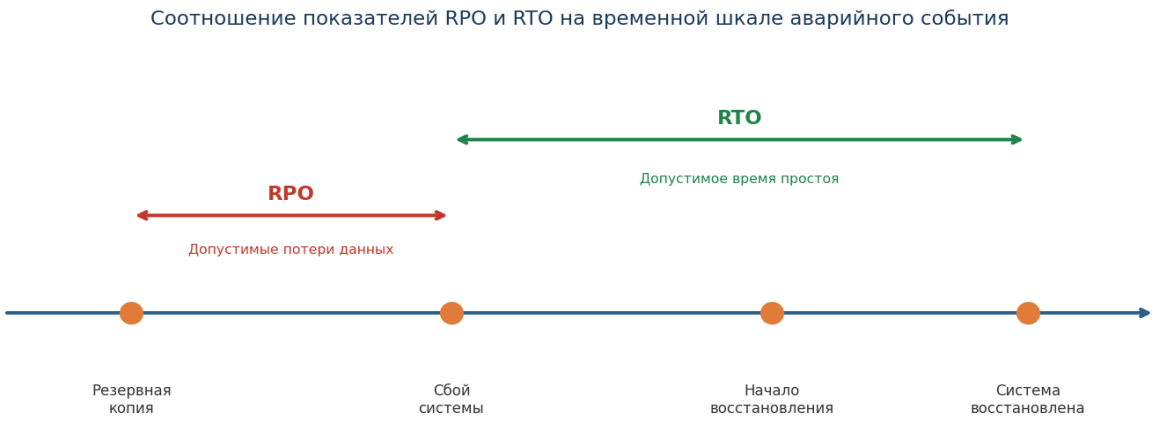

Рис. 1. Соотношение показателей RPO и RTO на временной шкале аварийного события (составлено автором на основе [10, 11])

Для SAP-систем на базе SAP HANA и Oracle целевые значения RPO и RTO определяются на основе анализа бизнес-влияния (Business Impact Analysis, BIA). В практике крупных производственных и торговых компаний типичные требования для ERP-систем выглядят следующим образом: RPO в диапазоне от 0 до 30 минут, RTO от 30 минут до 4 часов в зависимости от класса критичности системы и наличия горячего резервного узла. По данным Uptime Institute, около 60% крупных предприятий устанавливают для своих ERP-систем RTO не более двух часов [11].

Таблица 1. Классификация SAP-систем по требованиям RPO/RTO (составлено автором на основе [3, 10])

Класс критичности	**Целевой RPO**	**Целевой RTO**	**Типичные SAP-системы**
Tier 0 (критический)	менее 1 минуты	менее 15 минут	SAP HANA Production, финансовые модули
Tier 1 (важный)	1-15 минут	15-60 минут	SAP ERP Core, SCM, CRM
Tier 2 (значимый)	15-60 минут	1-4 часа	SAP BW, Solution Manager
Tier 3 (стандартный)	1-4 часа	4-24 часа	SAP DEV/QA среды, архивные системы

Важно понимать, что RPO и RTO не являются независимыми величинами. Снижение RPO требует повышения частоты резервного копирования или внедрения технологий непрерывной репликации, что увеличивает нагрузку на систему хранения и каналы передачи данных. Снижение RTO, в свою очередь,

требует либо использования горячего резерва (hot standby), либо оптимизации процедур восстановления, что влечёт дополнительные затраты на инфраструктуру. Задача инженера SAP-инфраструктуры состоит в нахождении экономически обоснованного баланса между этими метриками в рамках выделенного бюджета.

Понимание взаимосвязи RPO и RTO создаёт основу для следующего шага, а именно для рассмотрения технологической триады: резервного копирования, репликации и аварийного восстановления.

1.3. Взаимосвязь резервного копирования, репликации и аварийного восстановления

В современной практике управления данными SAP-систем используются три взаимодополняющих механизма: резервное копирование, репликация данных и аварийное восстановление как организационно-технический процесс. Их совместное применение образует многоуровневую систему защиты, способную удовлетворить требования к RPO и RTO различных классов критичности [12].

Резервное копирование обеспечивает создание периодических снимков состояния базы данных на внешних носителях. Оно является механизмом защиты от логических повреждений данных (ошибок приложений, случайного удаления), а также от физических катастроф. Основной характеристикой резервного копирования является то, что оно создаёт изолированную копию данных, не зависящую от состояния исходной системы. Для SAP HANA резервные копии создаются с использованием нативного интерфейса HANA Backup API или через интерфейс Backint, позволяющего интегрировать внешние системы резервного копирования, такие как Commvault, Veeam и NetBackup [13].

Репликация данных, в частности SAP HANA System Replication (HSR), обеспечивает синхронное или асинхронное копирование транзакционных данных на вторичный узел в режиме реального времени. В отличие от резервного копирования репликация не создаёт изолированных точек восстановления, но

позволяет достичь практически нулевого RPO для физических сбоев. Oracle Data Guard реализует аналогичный механизм для Oracle Database, обеспечивая непрерывное применение архивных журналов на резервном сервере [14]. Репликация не является заменой резервного копирования, поскольку логические повреждения данных немедленно распространяются на реплику.

Аварийное восстановление представляет собой задокументированный набор процедур, определяющих порядок действий персонала при наступлении различных аварийных сценариев. Оно опирается на оба технических механизма и включает не только технические шаги восстановления, но и организационные меры: оповещение персонала, переключение трафика приложений, верификацию восстановленных данных и отчётность.

Таблица 2. Сравнение механизмов защиты данных в SAP-инфраструктуре (составлено автором на основе [12, 14])

Механизм	**RPO**	**RTO**	**Защита от логических ошибок**	**Требования к хранилищу**
Резервное копирование	15 мин-8 ч	1-8 ч	Да	Высокие
Репликация (HSR/DG)	менее 1 мин	менее 15 мин	Нет	Средние
Снапшоты хранилища	5-60 мин	15-60 мин	Частично	Средние
Комбинированная защита	менее 5 мин	менее 30 мин	Да	Максимальные

Оптимальная стратегия защиты данных SAP-инфраструктуры, как правило, предполагает комбинирование всех трёх механизмов: репликация обеспечивает минимальный RPO для физических сбоев, резервные копии обеспечивают защиту от логических повреждений и долгосрочное хранение, а аварийное восстановление как процесс определяет порядок использования обоих механизмов в зависимости от характера аварии. Следующий подраздел посвящён специфике реализации всех указанных механизмов в конкретных платформах SAP HANA и Oracle.

1.4. Особенности защиты данных в средах SAP HANA и Oracle

SAP HANA и Oracle Database, несмотря на то что обе платформы относятся к классу реляционных СУБД корпоративного уровня, имеют принципиально различные архитектурные подходы к защите данных, что напрямую влияет на методику проектирования резервной инфраструктуры.

SAP HANA как in-memory база данных хранит рабочую копию данных в оперативной памяти и обеспечивает их персистентность через механизм savepoint-записи и журнал транзакций на диск. Savepoint (контрольная точка) создаётся каждые несколько минут и фиксирует согласованное состояние данных в памяти на диске. Пространство между двумя savepoint-записями покрывается журналом транзакций (HANA redo log). При создании полной резервной копии HANA последовательно сохраняет содержимое всех сервисов (indexserver, nameserver, xsengine) через Backup API, а затем фиксирует позицию в журнале [8, 15].

Интерфейс Backint for SAP HANA позволяет интегрировать специализированные системы резервного копирования, передавая им данные через стандартизированный канал. Это исключает необходимость промежуточного хранения резервной копии в локальной файловой системе и позволяет напрямую записывать данные в ленточные библиотеки, облачные хранилища (AWS S3, Azure Blob) или дедуплицирующие хранилища (Dell EMC Data Domain) [13].

Oracle Database реализует защиту данных преимущественно через механизм архивирования журнала повтора (Archive Log Mode) в сочетании с утилитой RMAN (Recovery Manager). RMAN обеспечивает создание полных, инкрементальных и архивных резервных копий с встроенной функцией контроля целостности блоков, дедупликации и каталогизации. Ключевой особенностью Oracle является поддержка инкрементальных копий уровня блока через функцию Block Change Tracking (BCT), которая значительно сокращает объём данных при инкрементальном резервном копировании [16].

Oracle Data Guard обеспечивает ведение физической резервной базы данных (physical standby) посредством непрерывного применения архивных журналов, полученных с основного сервера. В режиме Maximum Availability Data Guard гарантирует нулевые потери данных при синхронном подтверждении транзакций, что соответствует требованиям Tier 0 по RPO. Для архивирования резервных копий Oracle рекомендует применять политику Flashback Database в сочетании с хранением в Fast Recovery Area (FRA) [17].

Понимание платформенных особенностей SAP HANA и Oracle формирует необходимый фундамент для перехода к практическому проектированию стратегий резервного копирования, которому посвящён следующий раздел.

Раздел 2. Методика проектирования стратегии резервного копирования

2.1. Полные резервные копии: назначение, преимущества и ограничения

Полная резервная копия представляет собой снимок всей базы данных на момент выполнения операции и является базовым строительным блоком любой стратегии защиты данных. В контексте SAP HANA полная копия создаётся командой BACKUP DATA через HANA Backup API и включает все тома данных всех сервисов HANA-системы. Для Oracle Database аналогом является full database backup в RMAN, включающий все файлы данных, файл управления и параметрический файл spfile [15, 16].

Преимущество полной копии состоит в её самодостаточности: для восстановления из полного backup не требуются дополнительные файлы или журналы, кроме тех, которые необходимы для применения транзакций, произошедших после создания копии. Это упрощает процедуру восстановления и сокращает RTO по сравнению со сценариями, требующими применения цепочки инкрементальных копий. В ситуации критического аварийного восстановления, когда счёт идёт на минуты, простота процедуры имеет первостепенное значение [18].

Однако полные копии сопряжены с двумя существенными ограничениями. Первое касается объёма хранилища: полная копия занимает столько же места, сколько занимает сама база данных (с учётом применяемого сжатия). При ежедневном создании полных копий базы данных объёмом 10 ТБ с 7-дневным сроком хранения потребность в хранилище составит не менее 70 ТБ только под полные копии, не считая журнальных файлов. Второе ограничение касается нагрузки на систему: создание полной копии SAP HANA требует чтения всего объёма данных из памяти и их записи на диск, что при больших объёмах баз данных занимает несколько часов и создаёт дополнительную нагрузку на I/O-подсистему сервера [13, 19].

Оптимальная практика предполагает создание полных резервных копий SAP HANA и Oracle с периодичностью, устанавливаемой на основе анализа темпов изменения данных и требований к RPO. Как правило, для продуктивных систем Tier 1 полные копии выполняются еженедельно или раз в 2-3 дня, тогда как для систем Tier 0 с жёсткими RPO-требованиями они могут дополняться ежедневными инкрементальными или дифференциальными копиями. С полных копий начинается построение более сложной стратегии, рассматриваемой в последующих подразделах.

2.2. Инкрементальные резервные копии в модели оптимизации времени и объёма

Инкрементальная резервная копия фиксирует только те блоки данных, которые изменились со времени последней резервной копии любого типа (полной или инкрементальной). Данный подход существенно сокращает объём передаваемых и хранимых данных, однако усложняет процедуру восстановления: для восстановления к заданному моменту времени необходимо последовательно применить полную копию и всю цепочку инкрементальных копий вплоть до нужной точки [16].

SAP HANA поддерживает инкрементальные резервные копии начиная с версии HANA 2.0. Инкрементальная копия HANA фиксирует изменения в дельта-томах между двумя savepoint-записями. Для Oracle RMAN реализует инкрементальное копирование на уровне блоков данных с использованием функции Block Change Tracking (BCT): специальный файл BCT отслеживает, какие блоки были изменены с момента последнего резервного копирования, что позволяет читать только изменённые блоки без полного сканирования файлов данных [16, 20].

Модель оптимизации хранилища при использовании инкрементальных копий описывается следующим образом. Пусть объём полной копии базы данных равен V_{full} , ежедневный прирост изменённых данных составляет d% от V_{full}. Тогда объём ежедневной инкрементальной копии составит приблизительно

$V_{full} \times \frac{d}{100}$. При недельном цикле с одной полной и шестью инкрементальными копиями общий объём хранилища за неделю составит $V_{full} + 6 \times V_{full} \times \frac{d}{100}$, что при d = 5% равняется $V_{full} \times 1,3$. Аналогичный результат при ежедневных полных копиях потребовал бы $7 \times V_{full}$, то есть в 5,4 раза больше пространства [19].

Практический риск инкрементальных копий состоит в зависимости от целостности всей цепочки: повреждение любого звена цепочки делает невозможным восстановление ко всем точкам, следующим за ним. Во избежание этого риска рекомендуется периодически создавать полные копии, а также использовать функцию накопительного инкрементального backup в Oracle RMAN. После рассмотрения инкрементальных копий логично перейти к дифференциальным, занимающим промежуточное положение между полными и инкрементальными.

2.3. Дифференциальные резервные копии как компромиссный механизм

Дифференциальная резервная копия фиксирует все изменения, произошедшие с момента последней полной копии, независимо от того, сколько дифференциальных копий было создано за этот период. Принципиальное отличие от инкрементальной копии состоит в опорной точке: для инкрементальной копии это последняя копия любого типа, для дифференциальной – всегда последняя полная копия [18].

Это различие порождает компромисс: дифференциальные копии занимают больше места, чем инкрементальные (поскольку каждая следующая дифференциальная копия включает все изменения от последней полной, в том числе уже зафиксированные предыдущими дифференциальными копиями), однако обеспечивают существенно более простую процедуру восстановления. Для восстановления из дифференциального backup необходимы только

последняя полная копия и последняя дифференциальная копия, а не вся цепочка, как в случае с инкрементальными копиями.

В среде Oracle RMAN дифференциальный инкрементальный backup уровня 1 соответствует именно этой семантике: он захватывает все блоки, изменённые с момента последнего backup уровня 0 (то есть полного backup).

В SAP HANA понятие дифференциального backup также присутствует и поддерживается как отдельный тип резервного копирования. Дифференциальный backup сохраняет все изменения, произошедшие с момента последнего полного backup, независимо от наличия промежуточных инкрементальных или дифференциальных копий. [15, 20].

Дифференциальные копии особенно целесообразны в сценариях, где объём ежедневных изменений невелик (менее 20% от объёма базы данных), а требование к скорости восстановления (RTO) является приоритетным по сравнению с минимизацией хранилища. Это типично для OLTP-систем класса SAP ERP, где изменения носят транзакционный характер и затрагивают ограниченный набор таблиц. Ниже приведён радарный анализ, позволяющий наглядно сопоставить характеристики различных стратегий резервного копирования.

Выбор между дифференциальным и инкрементальным подходами должен основываться на анализе трёх факторов: скорости изменения данных в базе, требований к RTO и объёма доступного хранилища. При этом следует учитывать и четвёртый тип копий, обеспечивающий минимальные потери данных.

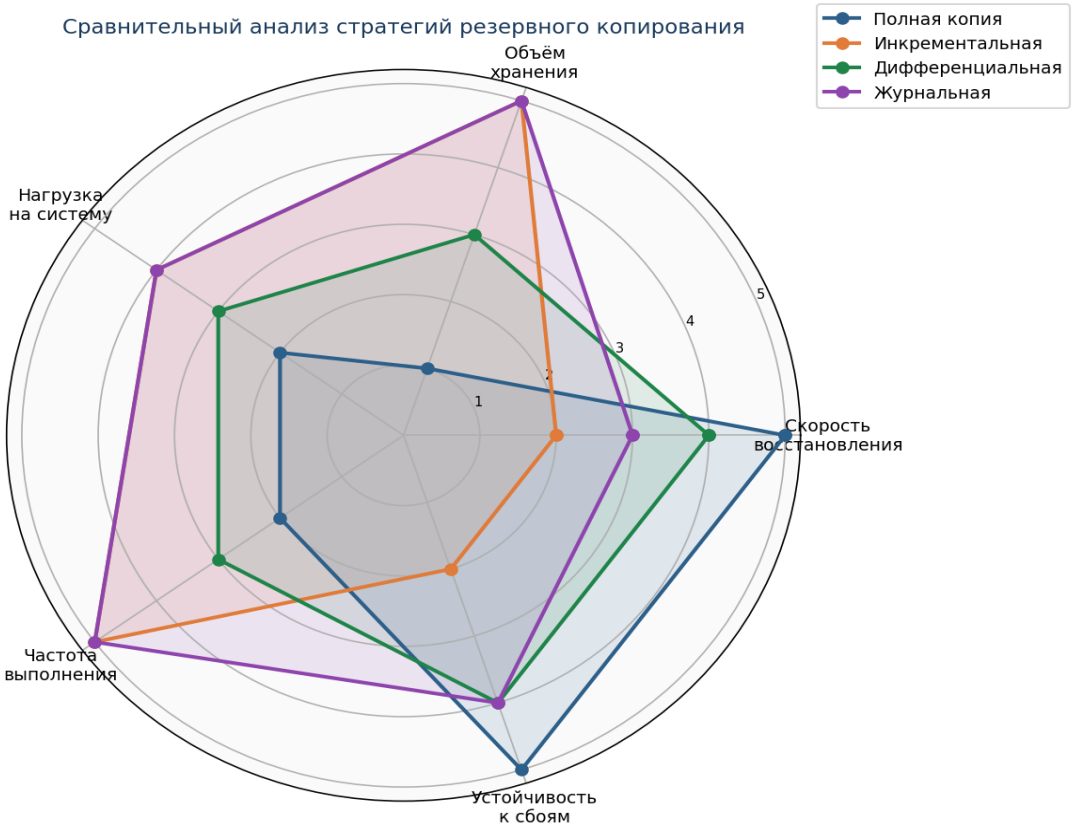

Рис. 2. Сравнительный анализ стратегий резервного копирования по ключевым параметрам (составлено автором на основе [12, 15, 18])

2.4. Журнальные копии и их роль в минимизации потерь данных

Журнальные резервные копии (log backups) занимают в стратегии защиты данных SAP-инфраструктуры особое место: именно они обеспечивают достижение RPO, измеряемого единицами или десятками минут. Журнал транзакций (redo log в SAP HANA, archive log в Oracle) фиксирует каждое изменение данных немедленно при его выполнении, что делает его источником для восстановления данных до произвольного момента времени в пределах периода хранения журналов [17].

В SAP HANA журнальные копии создаются автоматически в зависимости от значения определенного в параметре `log_backup_interval_mode`, при заполнении сегмента журнала либо по истечению интервала, или только по истечении интервала, задаваемого параметром `log_backup_timeout_s` в конфигурации global.ini. Рекомендуемое значение интервала для систем с RPO менее 15 минут составляет 5-15 минут. Журнальные сегменты автоматически записываются в каталог резервного копирования и могут быть отправлены через

Backint во внешнюю систему хранения. Для Oracle Database режим ARCHIVELOG обеспечивает автоматическое создание архивных журналов после заполнения оперативных redo log-файлов, а RMAN выполняет их регулярное резервное копирование [17, 21].

Важным аспектом управления журнальными копиями является политика их хранения. Хранение журналов должно охватывать весь период от последней полной резервной копии до текущего момента, а предпочтительно и несколько предыдущих циклов полного резервного копирования на случай повреждения полной копии. Расчёт объёма хранилища под журналы производится по формуле:

$$V_{log} = Rate_{change} \times T_{retention},$$

где:

$Rate_{change}$ – средний объём генерируемых журналов в час;

$T_{retention}$ – период хранения.

Для активных OLTP-систем SAP со скоростью генерации журналов 2-5 ГБ/час и периодом хранения 7 суток потребность составит от 336 до 840 ГБ только под журнальные файлы [19].

2.5. Выбор частоты выполнения копий для соблюдения целевых RPO/RTO

Частота выполнения резервных копий каждого типа непосредственно определяет достигаемые значения RPO и оказывает существенное влияние на RTO. Методика выбора оптимальной частоты базируется на анализе нескольких взаимосвязанных параметров: требований к RPO и RTO, объёма базы данных, скорости изменения данных, доступной полосы пропускания хранилища и допустимой нагрузки на продуктивную систему в период выполнения резервного копирования [22].

Для корректного отображения типового расписания резервного копирования SAP-системы следует разделять два операционных сценария: день выполнения полной резервной копии и день выполнения инкрементальной либо

дифференциальной копии. Журнальные копии при этом создаются непрерывно, как правило с заданным коротким интервалом, например каждые 15 минут, и обеспечивают постоянную защиту данных в течение всего 24-часового цикла. Инкрементальная или дифференциальная копия выполняется не в тот же день, что и полный бэкап, а в отдельные дни, когда полная резервная копия не запускается, компенсируя её отсутствие.

Рис. 3. Типовое расписание резервного копирования SAP-системы
с разделением дня полного бэкапа и дня инкрементального/дифференциального бэкапа
(составлено автором на основе [13, 22])

Алгоритм выбора частоты резервного копирования включает следующие шаги. На первом шаге определяется максимально допустимый RPO для данной системы. Именно RPO задаёт верхнюю границу интервала между журнальными копиями: интервал журнального backup не должен превышать целевое значение RPO. На втором шаге анализируется скорость роста объёма журналов: если при заданном интервале объём одной журнальной копии превышает 5-10 ГБ, интервал следует сократить во избежание чрезмерной нагрузки на I/O при восстановлении. На третьем шаге определяется частота полных и инкрементальных/дифференциальных копий исходя из допустимого времени

восстановления: чем реже создаются полные копии, тем длиннее цепочка журналов, необходимых для восстановления, и тем больше RTO. На четвёртом шаге производится верификация: суммарное время восстановления из полной копии и применения всех последующих журналов не должно превышать целевой RTO [23].

Выбранная частота резервного копирования напрямую влияет на объём требуемого хранилища, что составляет основу следующего раздела.

Раздел 3. Расчёт хранилища и прогнозирование роста резервной инфраструктуры

3.1. Методика расчёта объёма хранения под различные типы резервных копий

Расчёт требуемого объёма хранилища под резервные копии является обязательным этапом проектирования инфраструктуры защиты данных. Недооценка потребности в хранилище приводит к переполнению целевых каталогов, сбоям процессов резервного копирования и в конечном счёте к недостижению целевых RPO. Переоценка влечёт неоправданные капитальные и операционные затраты. Методика расчёта включает несколько составляющих, каждая из которых рассматривается ниже [19, 24].

Для расчёта объёма хранилища необходимо определить следующие исходные параметры: V_db – текущий объём базы данных, cr – коэффициент сжатия резервных копий, d – среднесуточный темп прироста данных (в процентах от V_{db}), r_{log} – средняя скорость генерации журналов (ГБ/час), T_{full} – период хранения полных резервных копий (дни), T_{log} – период хранения журнальных копий (дни), f_{full} – частота создания полных копий (раз в неделю).

Объём хранилища под полные резервные копии вычисляется по формуле:

$$V_{full\ store} = (\frac{V_{db}}{cr}) \times (\frac{T_{full}}{\frac{7}{f_{full}}})$$

При V_{db} = 10 ТБ; cr = 2; T_{full} = 14 дней; f_{full} = 1 раз в неделю значение составит: (10 / 2) × (14 / 7) = 10 ТБ. Объём под инкрементальные копии:

$$V_{incr\ store} = (\frac{V_{db} \times d}{100/cr}) \times (\frac{T_{full} - 7}{f_{full}})$$

Объём под журнальные копии:

$$V_{log\ store} = \frac{r_{log} \times 24 \times T_{log}}{cr}$$ [24].

В таблице 3 приведены результаты расчета потребности в хранилище для SAP-систем различного масштаба данных.

Таблица 3. Расчёт потребности в хранилище для SAP-систем различного масштаба (составлено автором)

Параметр	**Система A (10 ТБ)**	**Система B (50 ТБ)**	**Система C (2 ТБ)**
Объём БД (V_{db}, ТБ)	10	50	2
Коэффициент сжатия (cr)	2.0	2.5	1.8
Прирост данных/сут, %	3%	5%	2%
Скорость журналов, ГБ/ч	3	8	0.5
Хранилище под полные копии, ТБ	10	40	1.6
Хранилище под инкрементальные, ТБ	4.5	28	0.4
Хранилище под журналы (7 дней), ТБ	2.5	6.7	0.21
Итоговая потребность (14 дней), ТБ	17	74.7	2.2

Результаты расчёта демонстрируют, что потребность в хранилище под резервные копии, как правило, в 1.5-2 раза превышает объём самой базы данных при 14-дневном сроке хранения и применении компрессии. Это должно учитываться при планировании бюджета на инфраструктуру хранения на этапе проектирования SAP-ландшафта.

3.2. Учёт темпов роста базы данных при планировании ёмкости

Планирование ёмкости хранилища резервных копий должно учитывать не только текущий объём базы данных, но и прогнозируемый рост как самой базы, так и объёма резервных копий. Темп роста базы данных определяется двумя факторами: органическим ростом транзакционных данных и потенциальными изменениями в модели данных или масштабировании системы (подключение новых юридических лиц, расширение ассортиментных справочников, добавление новых модулей SAP).

Для корректного планирования рекомендуется собирать историческую статистику роста базы данных за период не менее 12 месяцев. В SAP HANA статистика хранится в системных представлениях M_DISK_USAGE и

M_DATA_VOLUME_STATISTICS. Для Oracle аналогичные данные содержатся в представлении DBA_SEGMENTS и таблицах AWR. На основе исторических данных выбирается модель роста: линейная (постоянный абсолютный прирост), экспоненциальная (постоянный процентный прирост) или ступенчатая (скачкообразный рост при плановых событиях расширения) [25].

Практика показывает, что для большинства зрелых SAP-систем с устоявшейся пользовательской базой темп роста транзакционных данных составляет 15-30% годовых, тогда как аналитические системы (BW/4HANA) могут расти значительно быстрее: 40-100% в год в активной фазе накопления исторических данных [3]. Использование SAP IQ (Sybase IQ) для архивирования исторических данных с переносом их из основной базы SAP HANA является распространённой практикой управления темпами роста хранилища резервных копий.

3.3. Моделирование потребности в хранилище на среднесрочном горизонте

Среднесрочное моделирование потребности в хранилище охватывает горизонт планирования от 12 до 36 месяцев и служит основой для инвестиционных решений по расширению инфраструктуры хранения. Для построения модели используются прогностические методы: экстраполяция текущих тенденций роста, сценарный анализ и метод Монте-Карло для оценки диапазона неопределённости. Ниже представлен график, демонстрирующий три сценария прогноза потребности в хранилище в зависимости от темпов роста базы данных на горизонте 24 месяцев.

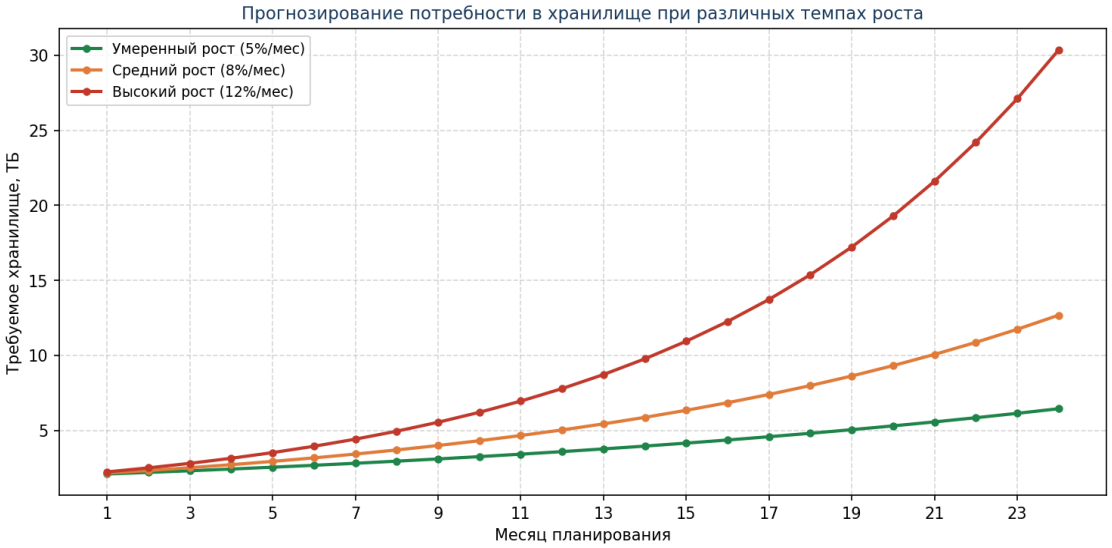

Рис. 4. Прогнозирование потребности в хранилище резервных копий при различных темпах роста (составлено автором)

Рекомендуемый подход к среднесрочному моделированию включает три сценария: базовый (исторический темп роста), оптимистичный (рост ниже исторического на 20%) и пессимистичный (рост выше исторического на 50%). Инфраструктурное решение принимается исходя из базового сценария с резервированием ёмкости до уровня пессимистичного сценария, что обеспечивает готовность к наиболее вероятному диапазону потребностей. Для SAP HANA Systems с использованием SAP HANA Dynamic Tiering часть данных может быть перенесена на более дешёвые уровни хранения, что существенно снижает стоимость хранения резервных копий в долгосрочной перспективе [26].

При построении модели необходимо также учитывать влияние жизненного цикла резервных копий на общий объём хранилища: введение политики автоматического удаления устаревших копий (retention policy) с помощью HANA Backup Catalog Management или Oracle RMAN Retention Policy позволяет удерживать занятое хранилище в заданных границах даже при росте базы данных.

3.4. Влияние окна резервного копирования на архитектуру хранилища

Окно резервного копирования определяется как временной интервал, в течение которого допустимо выполнение операций резервного копирования без существенного влияния на производительность продуктивной системы. Традиционно предпочтительным окном является ночное время (как правило, с 22:00 до 06:00), когда активность пользователей минимальна. Однако для глобальных компаний с круглосуточной транзакционной активностью понятие ночного окна фактически отсутствует, что требует проектирования архитектуры резервного копирования с минимальным влиянием на продуктивную нагрузку [23].

Размер окна резервного копирования непосредственно влияет на архитектурные решения по хранилищу. При узком окне (2-4 часа) для полного резервного копирования базы данных объёмом 10 ТБ необходима пропускная способность источника данных не менее 10 ТБ / 3 ч = 3.33 ТБ/ч или примерно 950 МБ/с. Это требует либо высокоскоростного SAN-подключения к хранилищу резервных копий, либо использования технологии параллельного резервного копирования через множество каналов (parallel backup channels в RMAN или несколько потоков Backint для SAP HANA) [13, 20].

Альтернативой является использование технологии снапшотов хранилища (storage snapshots), которые создают мгновенный снимок тома данных на уровне системы хранения, минуя СУБД. Для SAP HANA интеграция снапшотов реализована через механизм HANA Storage Snapshot, требующий выполнения команд PREPARE SNAPSHOT и CLOSE BACKUP соответственно до и после создания снимка. Снапшот создаётся практически мгновенно (несколько секунд вместо нескольких часов), однако хранение снапшотов на той же системе хранения, что и основные данные, не обеспечивает защиты от отказа самой системы хранения [8, 26].

Следовательно, оптимальная архитектура хранилища для SAP-систем с узким окном резервного копирования сочетает снапшоты для минимизации времени создания резервной копии с последующей асинхронной репликацией

данных снапшота на внешнее хранилище резервных копий. Это обеспечивает как высокую скорость создания копий, так и независимость от состояния основной системы хранения. Тем самым формируется технологическая база для перехода к разделу об аварийном восстановлении.

Раздел 4. Аварийное восстановление SAP-систем

4.1. Планирование сценариев утраты серверов и сервисов

Разработка плана аварийного восстановления (Disaster Recovery Plan, DRP) начинается с систематической каталогизации возможных сценариев сбоев, классифицированных по масштабу, причине и вероятности. Для SAP-инфраструктуры на базе SAP HANA и Oracle целесообразно выделять четыре основные категории сценариев: отказ отдельного компонента (сервер, диск, сетевой интерфейс), отказ сервиса (остановка SAP HANA indexserver, сбой слушателя Oracle Listener), отказ всей системы (полная недоступность продуктивного сервера) и катастрофа уровня ЦОД (пожар, наводнение, длительное отключение электроснабжения) [27].

Ниже представлена типовая архитектура аварийного восстановления SAP HANA, включающая основной и резервный ЦОД, механизм репликации и оркестрацию переключения.

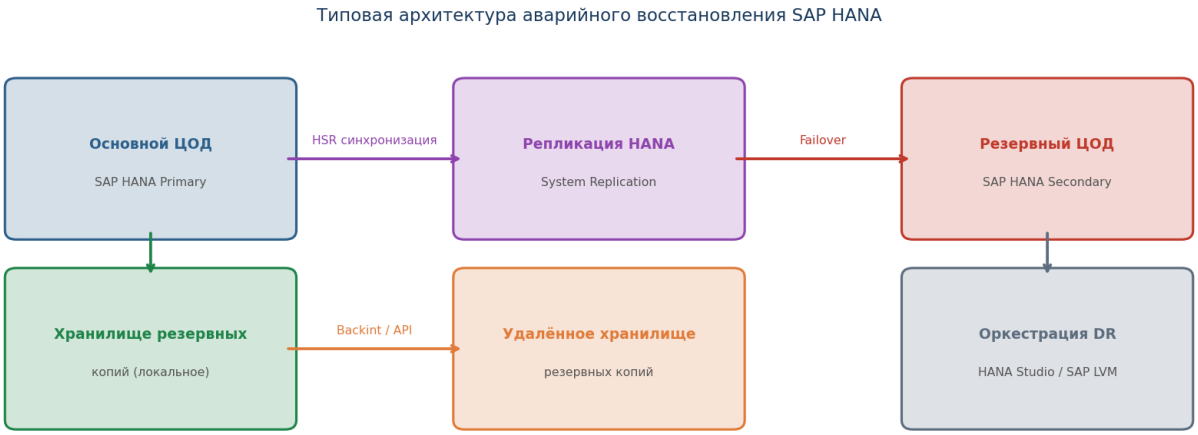

Рис.5. Типовая архитектура аварийного восстановления SAP HANA (составлено автором на основе [14, 27])

Для каждого сценария в DRP фиксируются следующие атрибуты: описание события-триггера, ожидаемые последствия для бизнеса, применимые технические механизмы восстановления, ответственный персонал, пошаговые инструкции по восстановлению и критерии успешного завершения. Особое внимание уделяется сценариям частичного отказа, когда SAP-система доступна,

но некоторые сервисы или модули работают некорректно: такие ситуации нередко сложнее диагностировать и устранять, чем полный отказ [28].

Для SAP HANA критическими сервисами, отказ которых требует немедленного реагирования, являются: indexserver (основной процессор запросов), nameserver (координатор кластера), preprocessor и xsengine (сервисы расширенного приложения). Для Oracle аналогичную роль выполняют: процессы PMON, SMON, DBWn, LGWR и CKPT. Матрица сценариев и рекомендуемых действий должна быть задокументирована в DRP в формате структурированных runbooks.

4.2. Порядок восстановления систем из резервных копий

Процедура восстановления SAP HANA из резервных копий следует чётко определённой последовательности шагов, каждый из которых требует верификации результата перед переходом к следующему. Отступление от установленного порядка или пропуск шагов верификации является одной из наиболее распространённых причин ошибок при восстановлении в реальных аварийных ситуациях, когда операторы действуют в условиях стресса и дефицита времени [29].

Стандартный порядок восстановления SAP HANA из резервных копий включает следующие этапы. На первом этапе выполняется подготовка целевой системы: проверка аппаратных ресурсов, установка программного обеспечения SAP HANA той же версии, что и источник, настройка параметров персистентности. На втором этапе производится восстановление системного тенанта (SYSTEMDB) из полной резервной копии с использованием SAP HANA Cockpit или hdbnsutil. На третьем этапе восстанавливаются пользовательские тенанты (tenant databases) в той же последовательности, что и их зависимости. На четвёртом этапе применяются журнальные копии для продвижения состояния системы к требуемой точке восстановления. На пятом этапе выполняется верификация: проверка целостности данных через HANA Studio, запуск тестовых транзакций SAP, сверка критических бизнес-данных [15, 29].

Для Oracle Database аналогичная процедура реализуется через RMAN restore и recover: команда RESTORE DATABASE восстанавливает файлы данных из backup set или backup piece, команда RECOVER DATABASE применяет архивные журналы до заданного момента времени (UNTIL TIME, UNTIL SCN или UNTIL SEQUENCE). Особое значение имеет использование каталога RMAN (RMAN Recovery Catalog) для хранения метаданных обо всех резервных копиях, что позволяет автоматически определять необходимый набор файлов для восстановления к любой заданной точке [30].

4.3. Роль репликации в сокращении времени восстановления

Технологии репликации данных занимают центральное место в стратегиях аварийного восстановления с минимальными значениями RTO. SAP HANA System Replication (HSR) обеспечивает синхронную или асинхронную репликацию на уровне слоя персистентности: все изменения данных передаются на вторичный узел в режиме, близком к реальному времени. При активации аварийного переключения (takeover) вторичный узел принимает роль основного, применяет последние полученные журналы и открывается для клиентских подключений. Типичное время полного переключения при использовании HSR в режиме synchronous in-memory (SYNCMEM) составляет менее 60 секунд [14].

Oracle Data Guard в режиме Maximum Performance обеспечивает асинхронную передачу архивных журналов на резервную базу данных с потенциальным отставанием от нескольких секунд до нескольких минут в зависимости от пропускной способности канала. В режиме Maximum Availability передача журналов осуществляется синхронно, что гарантирует нулевые потери данных, но требует подтверждения записи журнала на резервной базе до завершения транзакции. Active Data Guard позволяет резервной базе одновременно применять журналы и обслуживать запросы на чтение, что открывает возможность разгрузки продуктивной системы [17, 30].

С точки зрения аварийного восстановления принципиальная роль репликации состоит в устранении наиболее времязатратной части процедуры

восстановления: не требуется физического переноса данных из хранилища резервных копий на целевой сервер. Данные уже находятся на резервном узле в актуальном состоянии. Это позволяет достичь RTO менее 15-30 минут, что практически недостижимо при восстановлении из традиционных резервных копий для баз данных объёмом более 1 ТБ [28].

4.4. Тестирование процедур disaster recovery

Наличие документированного плана аварийного восстановления само по себе не является гарантией его работоспособности. Согласно данным Gartner за 2024 год, около 40% планов DR при первом реальном применении оказываются неполными или неактуальными: часть инструкций устарела после обновлений программного обеспечения, часть ресурсов оказывается недоступной, а часть ответственного персонала сменилась [3]. Регулярное тестирование процедур аварийного восстановления является единственным способом верификации их работоспособности.

Ниже представлена блок-схема процесса тестирования аварийного восстановления SAP-систем, отражающая последовательность этапов от планирования учений до обновления плана DR по их результатам (рис. 6).

Методология тестирования DR для SAP-систем включает несколько форматов, применяемых в зависимости от допустимого риска и доступности ресурсов. Настольные учения (tabletop exercises) не требуют реального переключения систем: команда DR последовательно обсуждает свои действия по каждому сценарию, выявляя пробелы в документации и распределении ответственности. Функциональное тестирование предполагает восстановление отдельной базы данных на изолированной тестовой системе из резервной копии для проверки целостности данных и работоспособности процедур восстановления. Полные учения DR (full DR drill) включают фактическое переключение на резервный ЦОД с измерением достигнутых RPO и RTO и проверкой работоспособности всего ландшафта SAP [27].

Рис. 6. Процесс тестирования аварийного восстановления SAP-систем (составлено автором на основе [27, 29])

Частота проведения учений DR должна соответствовать классу критичности системы: для систем Tier 0 рекомендуется не реже одного раза в квартал, для Tier 1 – не реже одного раза в полугодие. Каждое учение должно завершаться составлением детального отчёта с фиксацией реальных значений RPO и RTO, выявленных проблем и рекомендаций по улучшению.

4.5. Оценка качества плана аварийного восстановления по результатам учений

Оценка качества плана аварийного восстановления по результатам учений позволяет получить объективные данные о степени готовности организации к аварийным ситуациям и идентифицировать направления для улучшения. Методика оценки базируется на сравнении фактических и целевых значений

ключевых показателей: RPO, RTO, а также ряда дополнительных метрик, отражающих организационную составляющую DR [22, 29].

Ниже приведена сравнительная диаграмма, демонстрирующая типичное соотношение фактических и целевых значений RPO и RTO до и после проведения мероприятий по оптимизации плана DR на основе результатов учений.

Рис. 7. Сравнение показателей DR до и после оптимизации процедур (составлено автором)

Далее в таблице 4 будут описаны показатели качества плана аварийного восстановления.

Таблица 4. Показатели качества плана аварийного восстановления (составлено автором на основе [22, 29])

Показатель качества DR	**Формула расчёта**	**Целевое значение**	**Метод измерения**
Соответствие RPO	Факт. RPO / Целевой RPO	менее 1.0	Измерение временного разрыва при учениях
Соответствие RTO	Факт. RTO / Целевой RTO	менее 1.0	Хронометраж учений
Полнота документации	Кол-во покрытых сценариев / Всего сценариев	более 0.95	Аудит DRP
Актуальность runbooks	Кол-во актуал. инструкций / Всего	более 0.90	Ревью после обновл. ПО
Готовность персонала	Кол-во подготовл. спец. / Необходимо	более 0.85	Тестирование навыков

Для комплексной оценки качества DRP рекомендуется применять аддитивную взвешенную модель, в которой каждому показателю присваивается вес в соответствии с его значимостью для бизнеса. Совокупный индекс готовности к аварийному восстановлению (DR Readiness Index, DRRI) позволяет отслеживать динамику улучшений от учения к учению и обоснованно планировать инвестиции в совершенствование инфраструктуры и подготовку персонала. По результатам каждого учения план DR должен актуализироваться в части выявленных устаревших инструкций, уточнения контактных данных ответственного персонала и корректировки целевых значений RPO/RTO при изменении требований бизнеса.

Заключение

В рамках методического пособия была разработана комплексная методическая база для управления резервным копированием, аварийным восстановлением и контролем показателей RPO/RTO в SAP-инфраструктуре на базе SAP HANA и Oracle. Поставленная в аннотации цель достигнута: сформирована система методических рекомендаций, охватывающих все ключевые этапы жизненного цикла резервной копии: от концептуального обоснования и выбора стратегии до расчёта инфраструктуры хранения и верификации процедур восстановления.

Результаты работы позволяют сформулировать следующие авторские рекомендации для практикующих специалистов SAP-инфраструктуры. Первая рекомендация касается проектирования многоуровневой стратегии резервного копирования: для систем Tier 0 и Tier 1 следует сочетать HSR/Data Guard с журнальными копиями с интервалом 5-15 минут, еженедельными полными и ежедневными инкрементальными или дифференциальными копиями. Вторая рекомендация относится к расчёту хранилища: потребность следует рассчитывать с учётом прогноза роста на 24-36 месяцев, применяя пессимистичный сценарий в качестве проектного ориентира. Третья рекомендация связана с тестированием DR: минимальная допустимая периодичность функциональных учений составляет раз в полугодие для систем Tier 1, каждый квартал для Tier 0, с обязательным измерением фактических RPO и RTO.

Авторская гипотеза о возможности достижения RPO менее 15 минут и RTO менее 60 минут без пропорционального роста затрат подтверждается: применение технологии снапшотов в сочетании с HSR и журнальными копиями позволяет реализовать этот сценарий в рамках стандартного корпоративного бюджета на инфраструктуру хранения при условии правильного проектирования архитектуры и регулярного тестирования процедур восстановления.

Источники

1. Laudon K. C., Laudon J. P. Management Information Systems: Managing the Digital Firm. – 16th global ed. – Pearson, 2020.

2. IDC. The State of Disaster Recovery and Cyber-Recovery, 2024–2025: Factoring in AI [Электронный ресурс]. – 2025. – Режим доступа: https://www.idc.com/showcase/the-state-of-disaster-recovery-and-cyber-recovery-2024-2025-factoring-in-ai/ (дата обращения: 15.12.2025).

3. Gartner. Market Guide for Disaster Recovery as a Service [Электронный ресурс]. – 2024. – Режим доступа: https://www.gartner.com/en/documents/4224699 (дата обращения: 14.10.2025).

4. ISO 22301:2019. Security and resilience – Business continuity management systems – Requirements. – Geneva : International Organization for Standardization, 2019.

5. Nguyen N. D. K., Ali I., Gupta S., Chen R., Naresho B. S. Bridging the Nexus Between Cloud ERP and Enterprise Resilience // Journal of Global Information Management. – 2024. – Т. 32. – № 1. – С. 1–22. – DOI: https://doi.org/10.4018/JGIM.336556.

6. Magalhães A., Monteiro J. M., Brayner A. Main Memory Database Recovery: A Survey // ACM Computing Surveys. – 2021. – Т. 54. – № 2. – Ст. 46. – DOI: https://doi.org/10.1145/3442197.

7. ISO/IEC 27031:2025. Cybersecurity — Information and communication technology readiness for business continuity. – Geneva : International Organization for Standardization, 2025.

8. SAP SE. SAP HANA Administration Guide for SAP HANA Platform [Электронный ресурс]. – Version 2.0 SPS 08. – Режим доступа: https://help.sap.com/doc/eb75509ab0fd1014a2c6ba9b6d252832/2.0.08/en-US/SAP_HANA_Administration_Guide_en.pdf (дата обращения: 21.11.2025).

9. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector // Official Journal of the European Union. – 2022. – OJ L 333.

10. Ross R., Pillitteri V., Graubart R., Bodeau D., McQuaid R. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. – Gaithersburg, MD : National Institute of Standards and Technology, 2021. – DOI: https://doi.org/10.6028/NIST.SP.800-160v2r1.

11. Uptime Institute. Annual Outage Analysis 2024 [Электронный ресурс]. – 2024. – Режим доступа: https://uptimeinstitute.com/resources/research-and-reports/annual-outage-analysis-2024 (дата обращения: 27.11.2025).

12. Zhang Y., Zhong L., Yang S., Muntean G.-M. Distributed data backup and recovery for software-defined wide area network controllers // Transactions on Emerging Telecommunications Technologies. – 2022. – Т. 33. – № 4. – e4411. – DOI: https://doi.org/10.1002/ett.4411.

13. SAP SE. SAP HANA System Replication Guide [Электронный ресурс]. – Version 2.0 SPS 08. – Режим доступа: https://help.sap.com/doc/c81e9406d08046c0a118c8bef71f6bd/2.0.08/en-US/SAP_HANA_System_Replication_Guide_en.pdf (дата обращения: 18.11.2025).

14. Mergaerts M., Vanstechelman B. SAP HANA 2.0 Administration. – SAP PRESS, 2022.

15. SAP SE. SAP HANA Administration Guide for SAP HANA Platform [Электронный ресурс]. – Version 2.0 SPS 08. – Режим доступа: https://help.sap.com/docs/SAP_HANA_PLATFORM/6b94445c94ae495c83a19646e7c3fd56/15b4aa82ae7544f78f809e35add006ce.html?locale=en-US (дата обращения: 09.11.2025).

16. Oracle Corporation. Oracle Database Backup and Recovery User’s Guide, 19c [Электронный ресурс]. – 2025. – Режим доступа: https://docs.oracle.com/en/database/oracle/oracle-database/19/bradv/ (дата обращения: 03.12.2025).

17. Oracle Corporation. Oracle Data Guard Concepts and Administration, 19 c [Электронный ресурс]. – 2021. – Режим доступа: https://docs.oracle.com/en/database/oracle/oracle-database/19/sbydb/ (дата обращения: 24.09.2025).

18. Preston W. C. Modern Data Protection: Ensuring Recoverability of All Modern Workloads. – O'Reilly Media, 2021.

19. Müller H., Kharitonov A., Nahhas A., Bosse S., Turowski K. Addressing IT Capacity Management Concerns Using Machine Learning Techniques // SN Computer Science. – 2022. – Т. 3. – Ст. 26. – DOI: https://doi.org/10.1007/s42979-021-00862-8.

20. Oracle Corporation. Oracle Database Backup and Recovery Reference, 19 c [Электронный ресурс]. – 2025. – Режим доступа: https://docs.oracle.com/en/database/oracle/oracle-database/19/rcmrf/ (дата обращения: 12.12.2025).

21. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems – Requirements. – Geneva : International Organization for Standardization, 2022.

22. Whitman M. E., Mattord H. J. Management of Information Security. – 6th ed. – Cengage Learning, 2019.

23. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection – Information security controls. – Geneva : International Organization for Standardization, 2022.

24. NIST. The NIST Cybersecurity Framework (CSF) 2.0. – Gaithersburg, MD : National Institute of Standards and Technology, 2024. – DOI: https://doi.org/10.6028/NIST.CSWP.29.

25. Nelson A., Rekhi S., Souppaya M., Scarfone K. Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. – Gaithersburg, MD : National Institute of Standards and Technology, 2025. – DOI: https://doi.org/10.6028/NIST.SP.800-61r3.

26. Bauer N. SAP HANA Disaster Recovery with Storage Replication: Technical Report TR-4646 [Электронный ресурс]. – NetApp, 2020. – Режим доступа: https://www.netapp.com/media/8584-tr4646.pdf (дата обращения: 02.10.2025).

27. Lombard C. Mastering VMware Cloud Disaster Recovery and Ransomware Resilience: A Practical Guide on VMware Cloud Disaster and Ransomware Recovery SaaS Solution. – Apress, 2024.

28. Ross R., McEvilley M., Winstead M. Engineering Trustworthy Secure Systems. – Gaithersburg, MD : National Institute of Standards and Technology, 2022. – DOI: https://doi.org/10.6028/NIST.SP.800-160v1r1.

29. The Business Continuity Institute. Good Practice Guidelines (GPG) 7.0 [Электронный ресурс]. – 2023. – Режим доступа: https://www.thebci.org/certification-training/good-practice-guidelines.html (дата обращения: 10.12.2025).

30. Michalewicz M., Van Puymbroeck P. Oracle (Active) Data Guard 19c: Best Practices for a Selection of New Features [Электронный ресурс]. – Oracle White Paper, 2019. – Режим доступа: https://www.oracle.com/a/ocom/docs/adg-19c-new-features-5515417.pdf (дата обращения: 25.09.2025).

Методическое пособие

Семенков Александр Александрович

Управление резервным копированием, аварийным восстановлением и параметрами RPO/RTO в SAP-инфраструктуре на базе SAP HANA и Oracle

Подписано в печать 20.01.2026. Гарнитура Times New Roman.
Формат 60×84/16. Усл. п. л. 2,2. Тираж 500 экз. Заказ № 14/1.
Оригинал-макет подготовлен и тиражирован в ООО «ЭПИЦЕНТР»
308010, г. Белгород, пр-т Б. Хмельницкого, 135, офис 40
ООО «АПНИ», 308023, г. Белгород, пр-кт Богдана Хмельницкого, 135