УДК 654.026

**В.А. Бабошин, Ф.Ф. Сиротенко**

# НЕКОТОРЫЕ ВОПРОСЫ РАЗРАБОТКИ АРХИТЕКТУРЫ СИСТЕМЫ ХРАНЕНИЯ ДАННЫХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

***Бабошин Владимир Александрович,*** *окончил Ульяновское высшее военное командное училище связи им. Г.К. Орджоникидзе. Начальник отдела ОАО «НИИ «Рубин», к.т.н., доцент. Имеет статьи в области систем связи специального назначения, систем беспроводного доступа, систем хранения данных. [e-mail: boboberst@mail.ru].*

***Сиротенко Федор Федорович,*** *окончил Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича. Ведущий инженер ОАО «НИИ «Рубин». Имеет статьи в области систем управления сетями связи специального назначения, систем хранения данных. [e-mail: inforubin@rubin-spb.ru].*

Аннотация

В статье рассматриваются особенности разработки архитектуры системы хранения данных специального назначения, представлены подходы к разработке методики ее формирования.

Ключевые слова: единое информационное пространство, хранилище данных, модель миграции данных, протоколы хранения данных, виртуализация, облачные хранилища.

## Введение

В связи с дальнейшим развитием общества от индустриального к информационному происходит качественный рост объема передаваемой и хранимой информации как в государственной системе управления в целом, так и в системе управления Вооруженных Сил (ВС) РФ, что вызывает необходимость формирования единого информационного пространства государства (ЕИП). В частности, ЕИП ВС РФ представляет собой специальным образом упорядоченную и взаимосвязанную совокупность информационных, вычислительных и телекоммуникационных ресурсов, организованных и функционирующих во времени и пространстве (в космосе, воздухе, море и на суше) с целью повышения качества управления ВС и оружием в мирное и военное время [1]. Благодаря созданию ЕИП, достигается информационное превосходство на поле боя, что позволяет во много раз эффективнее реализовать боевой потенциал группировок войск (сил) в ходе военных действий. Техническую основу информационного пространства ВС РФ составляют различные инфокоммуникационные системы, представляющие собой совокупность автоматизированных цифровых сетей связи общего пользования и телекоммуникационных сетей с системами передачи и хранения данных, постро-

енных на основе конвергентных инфокоммуникационных технологий, объединенных системой управления и обеспечивающих предоставление пользователям услуг обмена, доступа, размещения и поиска информации различных типов в единой среде межвидового (межведомственного) вертикального и горизонтального электронного взаимодействия вне зависимости от места нахождения абонентов и информации [2].

Следует отметить, что рост объемов информации сопровождается отсутствием единых регламентов информационного обмена, разнообразием структур баз данных, межвидовой разобщенностью, разнообразием форм донесений, сводок и отчетов, что создает значительные трудности при формировании ЕИП ВС РФ.

Таким образом, создание комплексной системы хранения данных (СХД), являющейся основой ЕИП, – актуальная задача, включающая в себя две подзадачи, связанные, с одной стороны, с техническим аспектом создания хранилищ данных (ХД) как физических объектов и обеспечения их протокольного взаимодействия, с другой – с формированием среды доступа к данным для пользователей на основе виртуализации и создания облачных хранилищ.

## Структура и архитектура системы хранения данных

В качестве основы для формирования типовой архитектуры рассмотрим систему связи специального назначения, основой которой являются узлы специальной связи (УСС), объединенные между собой каналами и трактами, в том числе арендованными из единой сети электросвязи РФ (ЕСЭ РФ) [3]. Данная сеть функционирует на основе стека протоколов TCP / IP; принцип предоставления услуг основан на клиент-серверном взаимодействии. В сети реализована автоматизированная платформа управления со своей средой функционирования, а также система информационной безопасности, реализующая функции разграничения доступа к ресурсам сети и безопасной передачи информации. В качестве протокола управления используется протокол SNMP v. 2 (Simple Network Management Protocol) или CMIP (Common Management Information Protocol).

Системам хранения с непосредственным соединением DAS (Direct Attashed Storage) и построенным на их основе ХД свойственна ограниченная масштабируемость, сложность управления и опасность возникновения узких мест на серверах и в локальных сетях. Сетевые устройства хранения (файлеры) NAS (Network Attached Storage) поддерживают сетевую файловую систему и предоставляют доступ любому узлу сети. Стандартная сеть хранения SAN (Storage Area Network) обеспечивает резервные пути между клиентами и ХД, а также удаленное зеркалирование и резервное копирование, не снижающее производительность работы базовой сети, однако требует дополнительной инфраструктуры.

Таким образом, предметом архитектурной разработки является структура и архитектура отдельного кластера ХД, а также реализация процессов миграции данных как в рамках данного кластера (узла сети), так и при межкластерном (межузловом) взаимодействии. В качестве основного элемента СХД служит УСС, представленный в виде кластера (рис. 1) [4].

На рисунке 1 представлена децентрализованная комбинированная архитектура СХД кластера сети, элементами которой являются хранилища SAS (Serial Attashed Storage) или DAS (Direct Attashed Storage), а также NAS (Network Attashed Storage). Для каждого кластера создается общий дисковый массив NAS (RAID 5.0), а также ленточная библиотека SAS. Критичные данные резервируются в хранилищах смежных кластеров. В качестве физических носителей используются дисковые RAID-массивы и ленточные библиотеки. Уровни СХД и модель миграции данных представлены на рисунке 2.

Все хранилища, входящие в кластер, объединены на принципах виртуализации. Виртуализация ХД – это агрегирование множества физических устройств хранения данных с различными протоколами (SCSI, iSCSI или Fibre Channel) в единый виртуальный пул хранения, из которого, при необходимости, можно производить создание и инициализацию (provisioning) виртуальных томов хранения, отражающихся в плоскости управления сервера ХД в виде локально подключенных логических ХД. Данное решение позволяет создать такую виртуализированную среду, в которой администратор размещает ресурсы хранения на сервере приложений, воспринимающем эти ресурсы как реальное ХД, физически подключенное к нему, что упрощает процесс миграции данных и повышает надежность СХД в целом.

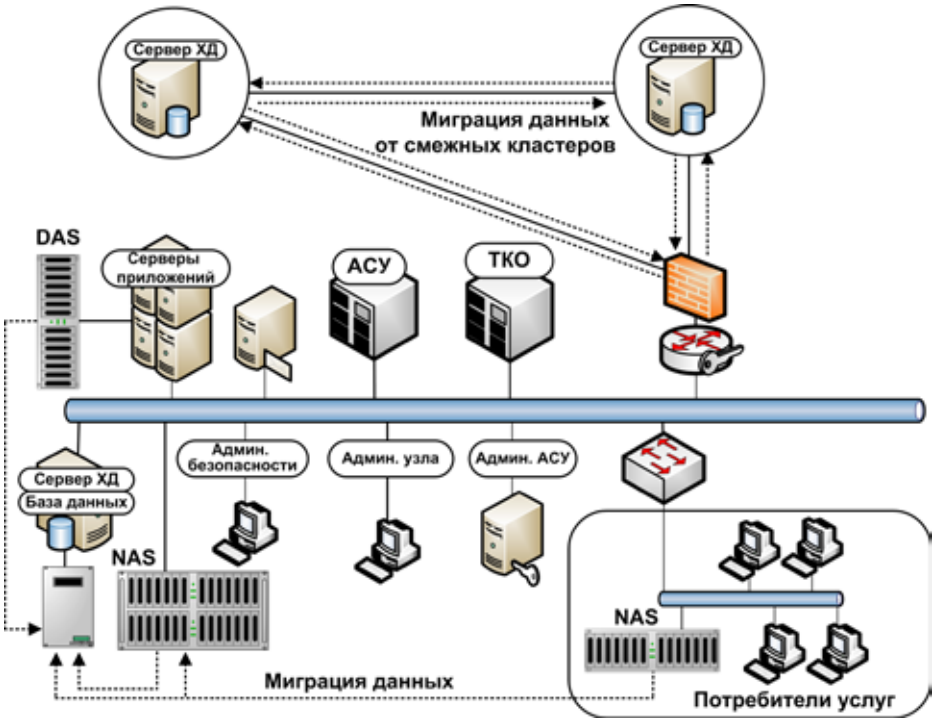


Рис. 1. Структура кластера СХД (вариант)

Данное решение основывается на открытых стандартах, оно независимо от производителей устройств, интерфейсов, протоколов соединения и платформ, что значительно упрощает процесс управления. То есть виртуализация создает среду, в которой каждая дисковая подсистема, вне зависимости от ее производителя, отображается на сервере хранения как устройство хранения, подключенное к нему непосредственно, что упрощает добавление и поддержку дополнительных устройств хранения. Прозрачная on-line миграция данных позволяет обслуживать и модернизировать устройства ХД, не прерывая работу приложений. Кроме того, можно динамически изменять права доступа к виртуальным томам, а также упрощается поддержка удаленного доступа к данным, резервного копирования, мирроринга и репликации.

Возможны два метода организации виртуализации: внеполосная (out-of-band) (ассиметричная) виртуализация и внутриполосная (in-band) (симметричная) виртуализация.

Внеполосная виртуализация реализуется контроллером метаданных, который размещается вне пути прохождения данных и действует как поставщик информации о размещении данных (mapping) между хостом и устройством хранения.

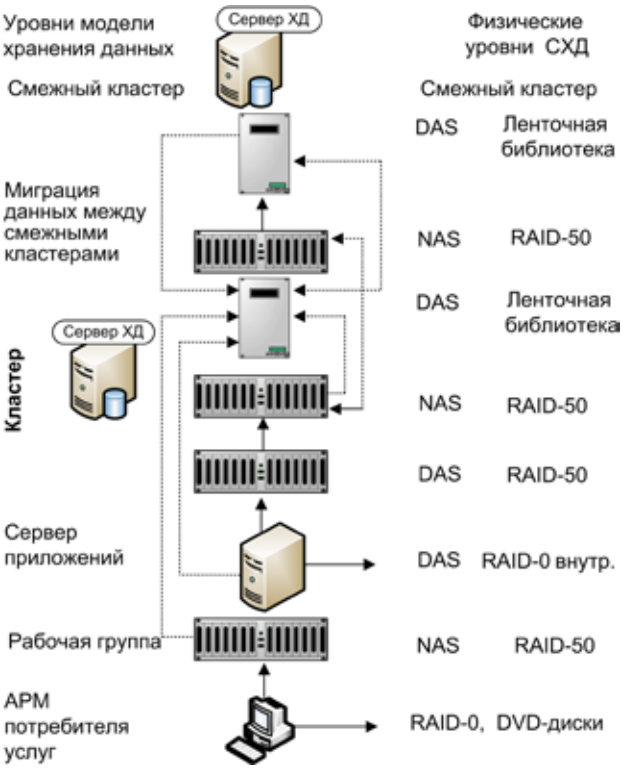


Рис. 2. Модель межкластерной миграции данных (вариант)

Внутриполосная виртуализация требует наличия центрального сервера хранения, который объединяет доступные ресурсы локально подключенных устройств хранения (DAS, SAN или NAS) в виде виртуальных томов и затем управляет хранением для всех серверов приложений. Он отвечает за повторную выдачу I/O запросов от серверов приложений к соответствующим устройствам хранения.

**Основные протоколы хранения данных**

Выбор стека протоколов для СХД должен базироваться на их кроссплатформенности, доступности и открытости, так как это связано с обеспечением информационной безопасности. Проведем краткий обзор некоторых основных протоколов.

1. Фактически виртуализация хранилищ, предоставляя возможность подключать виртуализированные тома ХД через IP-сети, послужила толчком к появлению IP Storage – технологии, которая поддерживает сетевые ХД с доступом на уровне блоков. Основное ее преимущество – расширенная совместимость и обеспечение межсетевого взаимодействия, а также создание SAN-сетей на базе единого стандарта, например Ethernet.

2. Известно, что для доступа к хранимым данным на уровне файлов применялись такие протоколы, как CIFS (Common Internet File System) и NFS (Network File System), поддерживающие запросы на уровне файлов данных на сервере, который управляет файловой системой (обычного файлового сервера или сетевого устройства хранения NAS). Различие между этими протоколами и протоколами IP Storage заключается в способе доступа к данным, который осуществляется на уровне файлов или блоков.

3. Высокоскоростной протокол передачи данных и одноименный интерфейс SCSI (Small Computer System Interface) представляют собой набор стандартов для физического подключения и передачи данных между компьютерами и периферийными устройствами.

4. Протокол и одноименный интерфейс SAS (Serial Attached SCSI) разработаны для замены параллельного интерфейса SCSI с целью обмена данными с жесткими дисками и ленточными накопителями, используют последовательный интерфейс для работы с DAS (непосредственно подключенными накопителями).

5. Дальнейшим развитием является протокол iSCSI (Internet Small Computer System Interface), иначе говоря, SCSI через IP, связывающий сервер с ХД через IP-сеть (рис. 3).

6. Протокол для высокоскоростной передачи данных FC (Fibre Channel). Его преимуществами являются высокая скорость, малая задержка и расширяемость (таблица).

7. Технология FCoE (Fibre Channel over Ethernet) используется в центрах обработки данных и позволяет использовать для передачи данных сети 10Gb Ethernet.

8. Протокол FCIP (Fibre Channel over Internet Protocol) обеспечивает соединение локальных портов Fibre Channel E-Port через инфраструктуру IP. Допускается воз-

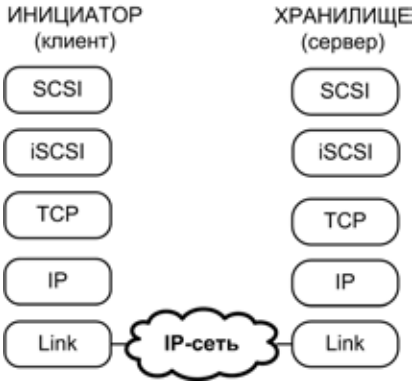


Рис. 3. Взаимодействие протоколов SCSI

можность сконфигурировать линки FCIP по схеме point-to-point без использования промежуточного оборудования IP-сети, и в этом случае физическую топологию можно рассматривать как использующую линки Fibre Channel ISL в качестве тунелей.

9. Протокол и одноименный последовательный интерфейс SATA (Serial ATA), разработанный для обмена данными с жесткими дисками (HDD и SSD).

10. Протокол и одноименная среда передачи данных Infiniband разработаны для обеспечения межсерверных соединений, в том числе и для организации RDMA (Remote Direct Memory Access). RDMA – группа протоколов, которые поддерживают передачу данных из памяти одного компьютера в память другого без буферизации в операционной системе, при этом исключается участие CPU в обработке кода переноса, данные пересылаются напрямую на соответствующий сетевой контроллер.

11. IPoIB (IP over Infiniband) – группа протоколов, описывающих передачу IP-пакетов поверх Infiniband:

– RFC 4390 Dynamic Host Configuration Protocol (DHCP) over InfiniBand;
– RFC 4391 Transmission of IP over InfiniBand (IPoIB);
– RFC 4392 IP over InfiniBand (IPoIB) Architecture.

12. Протокол и аппаратный интерфейс Thunderbolt (Intel) для подключения периферийных устройств к компьютеру с максимальной скоростью передачи до 10 Гбит/с по медному проводу и до 20 Гбит/с по оптическому кабелю.

13. Пакетная технология передачи данных 10Gb Ethernet включает в себя семь стандартов физической среды для LAN, MAN и WAN.

14. Протокол прикладного уровня Fast and Secure Protocol (FASP™) разработан для ускорения перемещения данных во избежание больших задержек RTT (Round Trip Time) и крупных потерь пакетов. Он базируется на протоколе UDP

Таблица

Многоуровневая модель протокола Fibre Channel

| Уровень | Функциональное назначение |
|---|---|
| FC-4 | *Протоколы прикладного уровня*<br>Инкапсуляция прикладных протоколов верхнего уровня (FICON, SCSI, IP, ATM) |
| FC-3 | *Общие сервисы*<br>Серверы имен, времени, ключей безопасности, управления |
| FC-2 | *Кадрирование и управление потоком*<br>Формирование фреймов и управление потоком данных |
| FC-1 | *Кодирование*<br>Кодирование и декодирование сигнала. Определение битовых ошибок. Синхронизация |
| FC-0 | *Физические интерфейсы*<br>Физические характеристики соединений, кабелей, коннекторов, сигнальные протоколы |

(User Datagram Protocol), который позволяет протоколу FASP определять RTT и частоту потери пакетов маршрута. Стеки протокола REST (Representational State Transfer) и FASP показаны на рисунке 4.

15. Защищенный сетевой протокол высокого уровня WebDAV (Web Distributed Authoring and Versioning) работает поверх HTTP. Используется в облачных хранилищах для доступа к объектам и коллекциям. Для хранения данных применяется большое количество серверов, но, с точки зрения пользователя, облако представляется как один сервер.

Рис. 4. Стек протокола FASP

**Последовательность формирования кластера системы хранения данных**

Структуризация процесса разработки СХД предполагает решение следующих задач:

– определение общего набора процессов, функций, задач управления хранением данных и его места в комплексе задач управления сетью;

– выделение специфичных задач разработки методов, знаний и стратегий управления для конкретных условий эксплуатации;

– представление процесса сбора и организации хранения данных в виде взаимосвязанного комплекса процессов, функций, задач и реализующих их моделей, методов, методик и алгоритмов.

В самом общем виде последовательность действий по формированию СХД состоит из следующих этапов:

1. Выбор обобщенной многоуровневой структуры СХД на основе кластеризации.

2. Обоснование физической реализации носителей данных и расчет объема ХД различных уровней СХД.

3. Обоснование архитектуры, выбор протоколов и принципов протокольного взаимодействия в процессе миграции, хранения и содержательной обработки данных с поддержкой технологии облачных хранилищ, в том числе и локальных.

4. Обоснование ресурса пропускной способности для обеспечения миграции данных.

5. Формирование структуры подсистемы управления СХД. В качестве основы системы управления (СУ) СХД предлагается использовать классическую схему «агент-менеджер», позволяющую строить распределенные СУ с рабочими местами, операторы которых могут соединяться с любым менеджером. В распределенных СУ используется несколько менеджеров, взаимодействующих друг с другом по одноранговой или иерархической схеме, которая соответствует стандартам *TMN (Telecommunication Management Network)* и является более эффективной.

6. Разработка обобщенного алгоритма процесса сбора и хранения данных как элемента подсистемы сетевого мониторинга.

Исходными данными являются:

– граф сети $G = (N, M)$, где $N = \{N_i\}$ – множество узлов специальной связи СССН, $M = \{m_{ij}\}$ – множество ветвей, $i, j = 1..N$;

$M = |m_{ij}|$ – структурная матрица ветвей / линий связи сети;

– множество контролируемых рабочих станций каждого узла $W_{sk}(N_i)$;

– множество пользователей услуг узла специальной связи $S_l(N_i)$;

– дисковая квота $D_t(N_i)$ для хранения технологической информации;

– дисковая квота $D_{см}(N_i)$ для хранения данных смежных кластеров;

– дисковая квота $D_{sl}(N_i) = S_l(N_i)d_{sl}$ для хранения данных пользователей $S_l$.

Определение общего объема ХД производится на основе выражения:

$$D_{СХД}(N_i) = D_t(N_i) + D_{CM}(N_i) + D_{Si}(N_i). \quad (1)$$

Кроме этого, после определения иерархии, количества и типа физических носителей хранилищ конкретного узла производится распределение требуемого объема (1) между хранилищами. При этом в зависимости от технологии реализации (RAID-массив, ленточная библиотека) хранилища вводится поправка на дополнительный технологический объем ХД. Для RAID-технологии полезный объем ХД равен:

$$DRAID = (n\text{-}1)*HDD_{size}, \quad (2)$$

где $n$ – число дисков в массиве, $D_{size}$ – размер диска.

В соответствии с предлагаемой моделью миграция данных происходит в зависимости от категории важности последовательно или напрямую в СХД высшего уровня иерархии [4], что требует определенного ресурса пропускной способности каналов и трактов сети. Полностью данную проблему можно решить при использовании технологии ХД SAN (Storage Area Network), однако в данном решении она применяться не будет, а в качестве каналов для обеспечения миграции данных СХД будет использоваться транспортная сеть.

## Заключение

Организация СХД на основе требований стандарта управления хранением данных Storage Management Initiative Standard (SMI-S) с использованием механизма виртуализации позволит реализовать совмещение логической (виртуальной) среды и физических устройств как в пределах одного кластера СХД, так и в облаках ХД в контексте формирования единого информационного пространства. Данное решение обеспечивает достаточно высокую надежность хранения данных, приемлемую скорость записи и выигрыш по времени доступа при распараллеливании запросов.

Таким образом, можно сформулировать основные критерии, которыми необходимо руководствоваться при создании современной системы хранения данных:

1. Открытая архитектура.

2. Масштабируемость.
3. Использование современных технологий хранения данных.
4. Обеспечение информационной и программной совместимости на всех уровнях иерархии.
5. Соответствие современным стандартам управления.
6. Гибкость стека протоколов.

## СПИСОК ЛИТЕРАТУРЫ

1. Копытко В.К., Шептура В.Н. Проблемы построения единого информационного пространства Вооруженных Сил Российской Федерации и возможные пути их решения. – ULR: http://www.avnrf.ru.

2. Легков К.Е. Цели и задачи создания инфокоммуникационной системы военного назначения // Актуальные проблемы информационного обеспечения деятельности Войск воздушно-космической обороны. – 2013. – № 1 – С. 22–30.

3. Бабошин В.А., Сиротенко Ф.Ф. Методы построения систем хранения данных в телекоммуникационной сети специального назначения // Вопросы радиоэлектроники. Сер. СОИУ. – 2012. – Вып. 2. – С. 29–44.

4. Бабошин В.А., Сиротенко Ф.Ф. Методика формирования системы хранения данных сети специального назначения // Вопросы радиоэлектроники. Сер. СОИУ. – 2013. – Вып. 1. – С. 32–41.

5. Бабошин В.А., Сиротенко Ф.Ф., Легков К.Е. Предложение по построению аппаратно-программного комплекса резервирования информации // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. – Ростов-на-Дону: ПЦ «Университет» СКФ МТУСИ, 2011. – С. 175–178.