УДК 004.04

Копейка О. В., к.т.н.
(Государственный университет телекоммуникаций, г. Киев. +380 (44) 249 29 23). okopiyka@gmail.com)

ПРОЕКТИРОВАНИЕ СЕРВИСОВ ИНФРАСТРУКТУРЫ ПРИЛОЖЕНИЙ В ДАТА-ЦЕНТРАХ

Копійка О. В. Проектування сервісів інфраструктури додатків в дата-центрах. Розглядаються питання побудови дата-центрів з сучасною архітектурою і наявністю повного обсягу сервісів. Сервіси управляють середовищем для виконування додатків, механізмами комунікацій між додатками і компонентами, інструментаріями контролю додатків і управління їх станом, а також сховищем для структурованих і неструктурованих типів даних. Визначений склад сервісів інфраструктури додатків, куди входять служби каталогів, бізнес додатків, інтеграції. Сформульовані основні вимоги до вказаних служб по наступних параметрах: доступність, безпека, масштабованість, керованість, консолідація і взаємодія.

Ключові слова: дата-центр, інфраструктура додатків, служби сервісів, каталог, бізнес додаток, інтеграція, доступність, безпека, масштабованість, керованість, консолідація

Копейка О. В. Проектирование сервисов инфраструктуры приложений в дата-центрах. Рассматриваются вопросы построения дата-центров с современной архитектурой и наличием полного объема сервисов. Сервисы управляют исполняемой средой для приложений, механизмами коммуникаций между приложениями и компонентами, инструментариями контроля приложений и управления их состоянием, а также хранилищем для структурированных и неструктурированных типов данных. Определен состав сервисов инфраструктуры приложений, в которую входят службы каталогов, бизнес приложений, интеграции. Сформулированы основные требования к указанным службам по следующим параметрам: доступность, безопасность, масштабируемость, управляемость, консолидация и взаимодействие.

Ключевые слова: дата-центр, инфраструктура приложений, службы сервисов, каталог, бизнес приложение, интеграция, доступность, безопасность, масштабируемость, управляемость, консолидация

Kopiyka O. V. Infrastructure applications services projection in the data centers. The article deals with the questions of data centers constructions with modern architecture and the presence of the full scope of services. These services controls executable application environment, communications mechanisms between applications and components, application's control tools and management of his condition, and stores for structured and unstructured data types. The composition of the application infrastructure services , which includes catalogue services, business applications, integrations. The main requirements for the specified services on the following parameters : availability, security , scalability, manageability , consolidation and cooperation.

Keywords: data center, infrastructure applications, catalogue, business applications, integrations, availability, security, manageability, consolidation and cooperation .

1. Введение и постановка задачи. В Украине уже 85% предприятий малого и среднего бизнеса используют тот или иной "облачный сервис". И это количество будет расти, так как сегодня облачные технологии предлагают практически безлимитные ресурсы бизнесу любого размера при стоимости, которая несопоставима с капитальными инвестициями в собственную инфраструктуру.

При реализации концепции "облачных сервисов" возникает задача построения дата-центров с современной архитектурой и наличием полного объема сервисов [1-11].

В современных дата-центрах выделяют следующие сервисы: сетевые; управления данными; управления ИТ-инфраструктурой; инфраструктуры приложений; безопасности.

В данной статье рассматриваются сервисы инфраструктуры приложений, которые состоят из службы каталогов; службы бизнес приложений; службы интеграции.

2. Служба каталогов. Служба каталогов обеспечивает иерархическую организацию информации отражающей ИТ-инфраструктуру корпорации для использования службами и пользователями. Функции службы каталога:

– обеспечение механизмов централизованной аутентификации пользователей, систем и авторизации их операций для защиты ИТ-ресурсов;

– хранение данных сервисов и приложений;

– хранение конфигурационной информации о настройке сервисов и приложений;

– обеспечение механизмов централизованного управления компонентами ИТ-инфраструктуры.

2.1. Логический и физический дизайн. Рассмотрим построение сервиса каталогов на примере вымышленной всеукраинской корпорации NameCorp (single forest).

Дизайн доменов. Доменная модель одного глобального региона (global regional domain model) содержит два домена (Рис. 1): *корневой* домен NameCorp.net, содержащий записи сервисных специалистов, и *дочерний* домен corp.NameCorp.net, содержащий записи всех пользователей, компьютеров и групп корпорации.

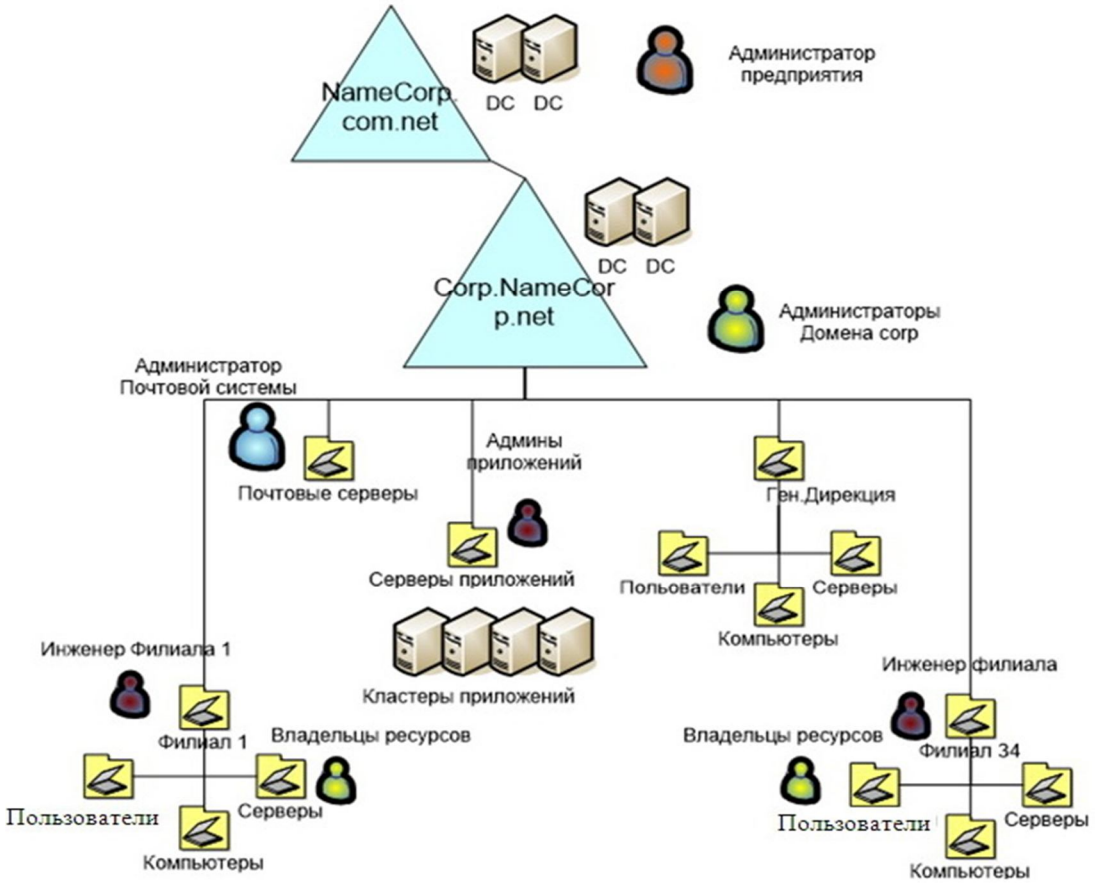

Рис. 1. Организация сервиса каталога в корпорации

Возможно создание домена test.NameCorp.net и использование его для тестирования и подготовки к вводу в эксплуатацию новых систем и релизов.

DNS архитектура. Служба DNS интегрирована с Active Directory.

Иерархия Organization Units (OU). Объекты OU отражают географическую модель корпорации на верхнем уровне иерархии и объектную модель на нижних уровнях иерархии (Рис. 2).

Иерархия OU должна обеспечить с одной стороны независимую работу 6 основных групп администраторов и более 400 специалистов во всех подразделениях корпорации, с другой эффективное использование групповых политик конфигурации рабочих мест и систем. Для этого верхние контейнеры отражают иерархию групп администрирования центра обработки данных (ЦОД), пользователей, а вложенные контейнеры содержат объекты управления – серверы, рабочие станции, пользователей и группа безопасности.

Топология сайтов. Шесть площадок, топология репликации базируется на физической топологии сети передачи данных (DPT каналы).

Размещение контролеров домена. Служба каталога разворачивается на 14 контроллерах домена. Киевский ЦОД 1 содержит два контроллера домена NameCorp.net и два контроллера домена corp.NameCorp.net. В остальных пяти ЦОД имеется по два контролера домена corp.NameCorp.net.

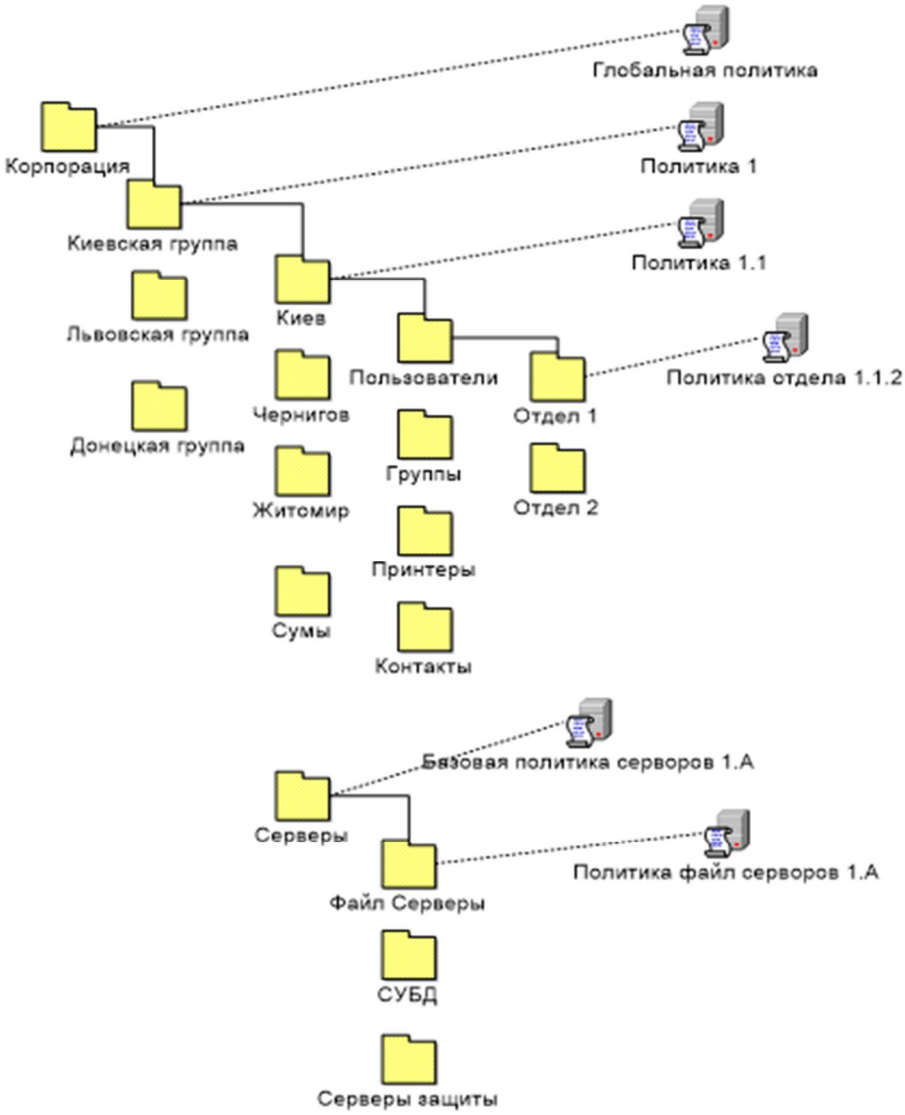

Рис. 2. Иерархия объектов в каталоге корпорации

2.2. Режим работы службы каталога Windows Server.

Серверное обеспечение. В системе имеется 14 серверов Windows Server Standart. Серверы двух процессорные с 2 Гб памяти и 16 Гб дискового пространства. Пять дисковых массивов: 1) RAID 1 для операционной системы, 2) RAID 1 для журнала AD, 3) RAID 0+1, 4) для базы данных AD, 5) для базы данных SYSVOL.

Сеть хранения данных. – Службой не используется.

Коммуникационная сеть. Для обеспечения работы службы в ЦОД настраиваются:

– коммутатор внутренней интеграции, используются функции VLAN и Firewall;

– центральный коммутатор ЦОД, используются функции VLAN и Firewall;

– коммутатор периметра, используются функции VLAN и Firewall;

– оборудование границы сети.

Доступность обеспечивается с помощью дублирования серверов и регистрации их служб в системе DNS. Дублируются также аппаратные компоненты серверов, в частности сетевые адаптеры.

Безопасность. Для работы со службой каталога Active Directory нескольких административных групп используются механизмы делегирования разрешений. Работа с группами Enterprise и Domain Administrators а также с учетной записью Administrator ведется через журнал регистрации операций.

Масштабируемость. 12 домен контроллеров достаточно для обслуживания запросов от 60000 пользователей. Если количество пользователей значительно возрастет, служба может быть масштабирована путем добавления дополнительных контролеров домена.

Управляемость. Для управления службой каталога в терминах MOF выделяются пять ролей (Табл. 1). Управление осуществляется набором графического инструментария MMC и набором командного инструментария adminpack.msi, support tools.

Консолидация и взаимодействие. Служба консолидирована со службой DNS.

Роли в службе управления каталога **Табл. 1**

Имя роли	Задачи роли	Active Directory разрешения
Владелец леса: администратор компании	Контроль конфигурации службы каталога.	Enterprise Admins
Владелец леса: администратор схемы	Контроль конфигурации схемы службы каталога.	Schema Admins
Владелец топологии репликации	Обеспечение работы сервиса и контроль репликации. Модернизация топологии в соответствии с модернизацией сети. Перемещение объекта контролера домена в другие сайты и сети. Поддержка сетевой карты Корпорации. Взаимодействие с сетевой группой.	Глобальная группа созданная в корневом домене леса и с полными разрешениями на объекты сайтов.
Владелец домена	Управление доменом Управление операциями с контролером домена Мониторинг «здоровья» Управления системными службами. Резервное копирование и восстановление Создание объектов и политик. Делегирование полномочий Создание OU	Domain Admins
Владелец OU`	Управление иерархией в OU	Группа с правами на OU и вложенные обьекты.

3. Службы бизнес приложений (ERP, CRM, Exchange, SharePoint, Live Communication Server, Content Management Services)**.** Рассмортим приципы построения службы бизнес приложений на примере всеукраинской корпорации.

3.1. Структура службы. Основные бизнес приложения корпорации включают в себя следующие компоненты:

1. Система коммуникаций на базе Exchange, Live Communication Server и Office.
   1.1. Электронная почта.
   1.2. Персональные и общие календари.
   1.3. Назначение заданий и контроль выполнения.
   1.4. Корпоративные адресные книги.
   1.5. Система контроля присутствия человека.
   1.6. Мгновенные сообщения.
   1.7.Аудио конференции.
   1.8. Видеоконференции.
2. Система коллективной работы на базе иерархии порталов SharePoint.
   2.1. Тематическое хранилище файлов и информации.
   2.2. Коллективная работа с документами.
3. Система управления проектами.

***Коммуникационная система Exch*ange** (Рис. 3) включает в себя компоненты:

1. Сервера Интернет доступа – отвечают за работу с почтой полученной из публичной сети, выполнение функций защиты от вирусов и спама.

2. Сервера центральной маршрутизации – отвечают за маршрутизацию сообщений внутри Корпорации.

3. Сервера клиентского доступа – отвечают за работу с клиентами, выполение функции шифрования и цифровой подписи сообщений

4. Сервера обслуживания почтовых ящиков.

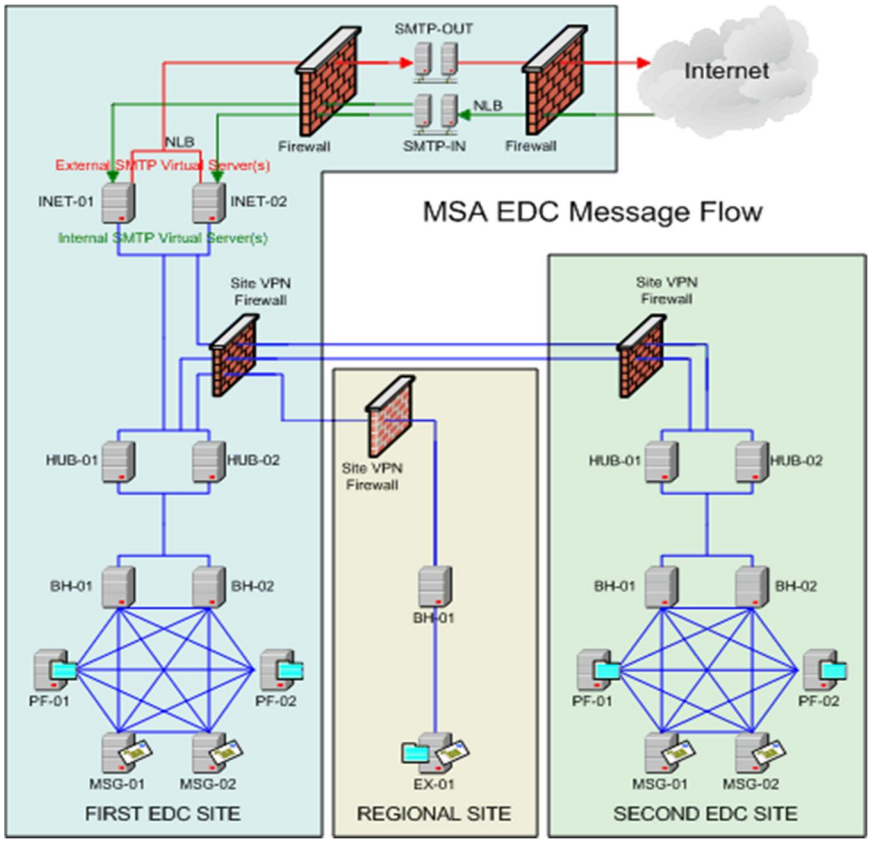

Рис. 3. Exchange в службе бизнес приложений корпорации

Система коммуникаций в режиме реального времени включает в себя два компонента

1. Центральный сервис Live Communication Server (LCS).
2. Серверы маршрутизации LCS, развернутые вокруг центрального.

Безопасность и адресные книги интегрированы в Active Directory корпорации.

На рабочих местах установлено приложение Messenger. Сотрудник персонально выбирает подчиненных или партнеров для взаимодействия.

Система коллективной работы развернута на базе пяти систем коллективной работы SharePoint Portal Server. Каждая система поддерживает несколько тысяч порталов. Логически порталы коллективной работы отражают организационную структуру и обеспечивают площадки для отделов, проектов и процессов корпорации. Порталы типизированы:

1. Портал подразделения – содержит каркас и информацию отображающую работу подразделения или отдела.
2. Портал рабочей группы – содержит информацию для коллективной работы группы сотрудников.
3. Портал библиотеки – содержит справочную информацию или тематическую библиотеку.
4. Портал процесса – содержит информацию о состоянии процесса, поддерживаемого рабочей группой.
5. Портал проекта – содержит файлы и информацию по проекту, используемые проектной группой.
6. Персональный портал сотрудника – содержит общую информацию о сотруднике.

3.2. Физическая организация.

Серверное обеспечение. Exchange разворачивается на 22 серверах маршрутизации уровня HP DL 380 (2 процессора, 2Гб памяти, RAID 1 – 16 Гб) и 20 серверах хранения уровня HP DL 380 (4 процессора, 8 Гб памяти, RAID 1 – 16 Гб). Используется технология NLB и fail-over кластеризации. LCS разворачивается на шести серверах уровня HP DL 380.

SharePoint использует пять серверов – по одному в каждом ЦОД. SharePoint использует службу управления хранением данных на базе MS SQL Server.

Сеть хранения данных обеспечивает 300 Мб пространства для каждого почтового ящика. SAN в каждом ЦОД должна обладать емкостью 10 Тб.

Коммуникационная сеть. Для обеспечения работы службы в ЦОД настраиваются элементы комуникационной сети аналогично п. 2.2.

Доступность обеспечивается использованием технологии кластеризации.

Безопасность. Аутентификация и авторизация с помощью Active Directory. Для сообщений и документов применяются технологии криптографичекой защиты и цифровой подписи. Коммуникации шифруются внутренними средствами. Системы коммуникаций дополнительно устанавливают модули антивирусной защиты.

Масштабируемость. При необходимости службу можно масштабировать горизонтально, путем добавления серверов и расширения сети хранения данных.

Управляемость. Для управления службой каталога в терминах MOF выделяются пять ролей по аналогии с организацией команды управления службы управления данными.

Консолидация и взаимодействие. Служба интегрирована со службами каталога Active Directory, управления сертификатами PKI, защиты периметра и управления.

4. Службы интеграции (BizTalk, .NET Frameworks, COM+, MSMQ). Роль информационных технологий внутри корпорации включает не только решения оптимизации расходов на выполнение набора бизнес операций или процессов, но непосредственное увеличение доходов и прибылей компании. Такое смещение фокуса требует быструю и эффективную интеграцию информации и процессов с поставщиками, партнерами заказчиками (Рис. 4).

4.1. Общий подход для решения задачи интеграции основывается на двух решениях (Рис. 5):

1. Использование архитектуры **Web сервисов**, обеспечивающий создание и эффективную работу связанных (loose coupling) приложений.
2. Использование серверов интеграции приложений BizTalk, как системы централизованного описания, реализации и сопровождения интеграционных взаимосвязей.

Требования к приложениям, которые будут создаваться и вводиться в эксплуатацию, обязательно включают реализацию в соответствии со стандартами Web-сервисов (http://w3c.org). Из двух платформ построения приложений/web-сервисов – диалект IBM J2EE и платформа Microsoft.NET, корпорация может ориентироваться на платформу .NET (http://www.forrester.com/Research/Document/Excerpt/0,7211,35261,00.html и http://middleware-company/j2eedotnetbench).

В информационной системе предприятия у каждого существующего приложения есть собственный протокол для обмена данными. Базовые средства BizTalk Server включают инфраструктуру передачи сообщений, обладающую возможностью обмена данными с практически любым приложением корпорации. В информационной среде с несколькими бизнес приложениями, ни одно отдельное приложение не имеет сведений о бизнес-процессе в целом. Бизнес-процесс, а также сведения, необходимые для координации всех его составляющих, реализуется в приложении BizTalk Server.

Важной задачей является интеграция приложений внутри одной организации, но интеграция приложений на уровне разных организаций, когда в автоматизации процессов задействованы системы компаний-контрагентов, может представлять для бизнеса еще большую ценность.

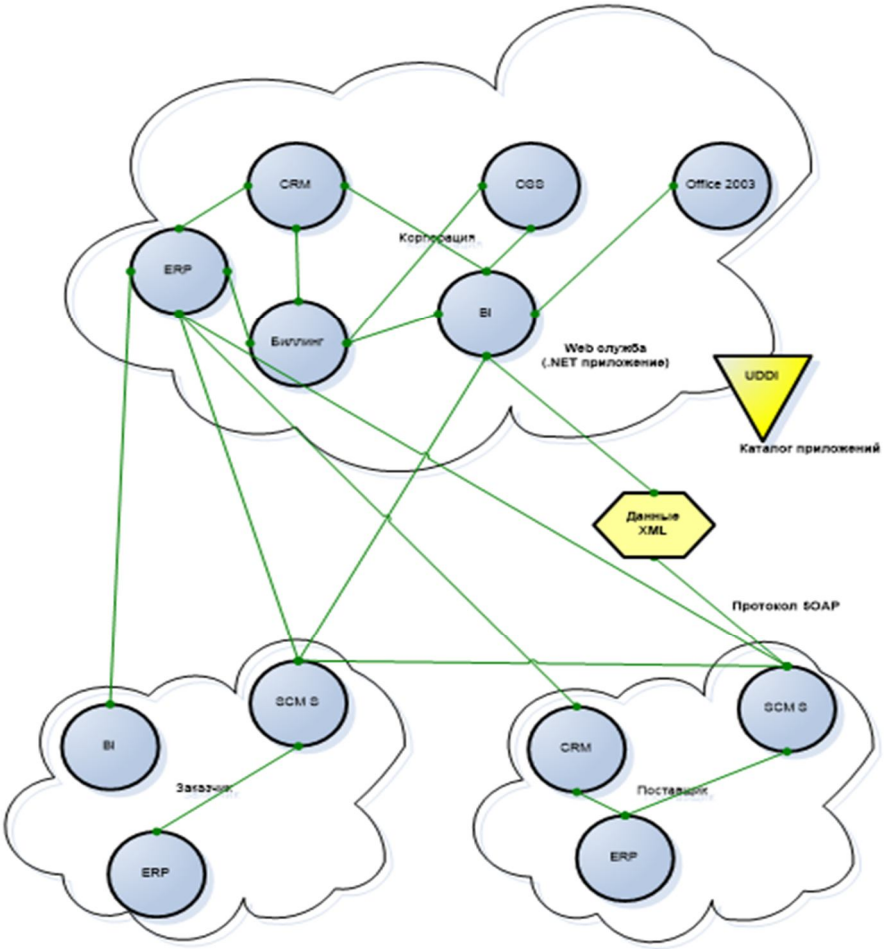

Рис. 4. Существующие информационные потоки в Корпорации

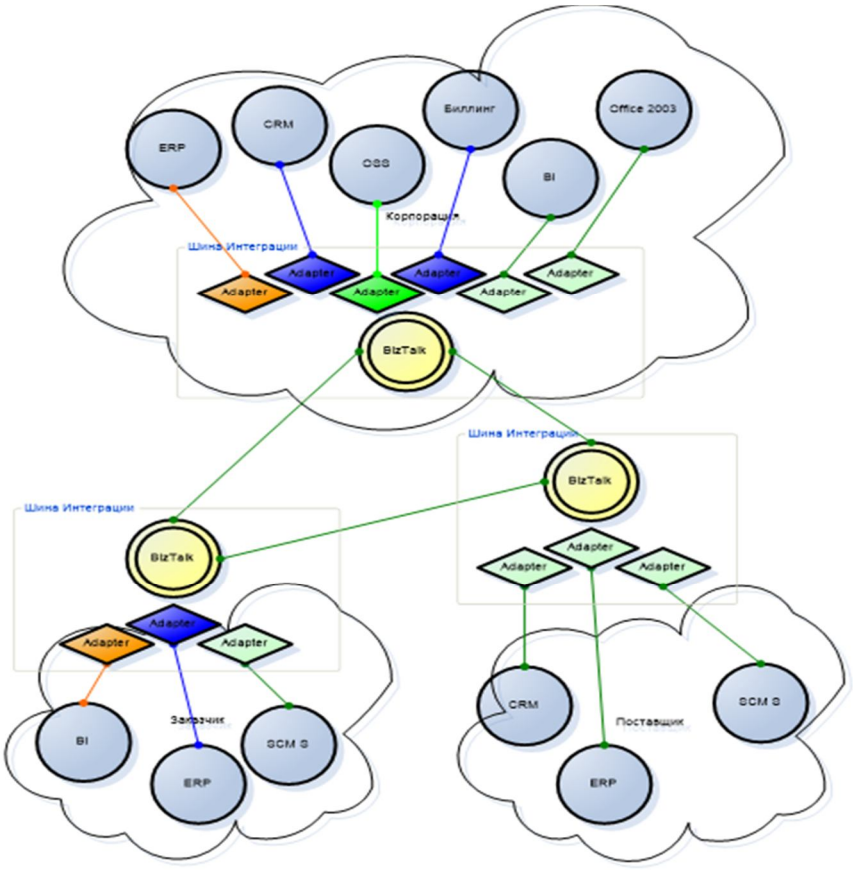

Рис. 5. Информационные потоки в службе интеграции корпорации

4.2. Логическая организация. Инфраструктура Web служб состоит из следующих компонентов:

1. .NET Framework – среда исполнения web сервисов. Среда исполнения устанавливается на все сервера и рабочие станции в Корпорации. Управление версиями и обновлениями обеспечивается системами управления (SMS).

2. Сервер приложений Internet Information Server – сервер приложений, сервер каталога UDDI и др. Сервер приложений обеспечивает слой бизнес-логики корпоративных многоуровневых приложений.

3. Компонент универсального доступа к данным – MDAC.

4. Универсальная шина интеграции на базе BizTalk – сервер обеспечения надежного транспорта, управления сверхдлинными транзакциями и бизнес логикой интеграции приложений (integration orchestration).

5. Адаптеры BizTalk – интерфейсы (программные модули сервера BizTalk) очистки и преобразования информации для подключения приложения к шине. (SAP adapter, SWIFT adapter, EDIFACT адаптер и более 500 др.).

Шина интеграции разворачивается в каждом ЦОД и обеспечивает взаимодействие, как с собственными внутренними приложениями, так и с внешними – партнерскими.

4.3. Физический дизайн.

Серверное обеспечение. BizTalk разворачивается на двух 2х кластерах (2 процессора, 4Гб памяти, RAID 1 – 16 Гб) в каждом ЦОД. Один кластер обеспечивает поддержку процессов – Virtual BizTalk Messaging и Virtual Message Queuing Instance. Второй кластер обеспечивает поддержку также следующих процессов – Virtual BizTalk Orchestration, Virtual WebDAV Instance. Сервер BizTalk использует сервис управления данными (MS SQL).

Сеть хранения данных – обеспечивает хранение очередей BizTalk.

Коммуникационная сеть. Для обеспечения работы службы в ЦОД настраиваются элементы комуникационной сети аналогично п. 2.2..

Доступность обеспечивается технологией кластеризации, горячей заменой и восстановлением из резервной копии. Служба управления данных и SAN отвечает за доступность данных.

Безопасность. Аутентификация и авторизация осуществляется с помощью Active Directory. Предусматривается использование кросс-корпоративных систем PKI.

Масштабируемость. Сервис поддерживает горизонтальной и вертикальное масштабирование.

Управляемость. Для управления службой в терминах MOF выделяются пять ролей по аналогии с организацией команды управления службы управления данными. Сервис требует наличие системы управления (в частности MOM и SMS) для обеспечения своей эксплуатации.

Консолидация и взаимодействие. Служба интегрирована со службой каталога Active Directory, службой управления сертификатами PKI, службой защиты периметра, службой управления данными и бизнес приложениями.

Выводы. В статье рассматривается задача проектирования сервисов инфраструктуры приложений в дата центрах, которые определяются в соответствии с архитектурой инфраструктуры приложений. Эти сервисы управляют исполняемой средой для приложений,

механизмами коммуникаций между приложениями и компонентами, инструментариями контроля приложения и управления его состоянием, а также хранилищем для структурированных и неструктурированных типов данных.

Определен состав сервисов инфраструктуры приложений, в которую входят следующие службы: каталогов, бизнесс приложений, интеграции.

Сформулированы основные требования к указанным службам по следующим параметрам: доступность, безопасность, масштабируемость, управляемость, консолидация и взаимодействие.

Литература

1. Еталонні архітектури MSA. – К.: Майкрософт Україна; К.: Видавнича група BHN, 2005. – 352 с.

2. Копейка О. В. Сетевые службы и службы сетевых устройств в Дата-центрах / О. В. Копейка // Системи управління, навігації та зв'язку. – 2013. – Випуск 4 (28). – С. 98-104

3. Копейка О. В. Архитектура системы управления ИТ-инфраструктурой в современных дата-центрах / О. В.Копейка // Наукові записки Українського науково-дослідного інституту зв'язку. – 2014. – №1(29). – С. 29-37

4. Довгий С. О. Засади регіональної інформатизації / С. О. Довгий, О. В. Копійка, Ю. Т. Черепін. – К.: ВПЦ «ТИРАЖ», 2004. – 304 с.

5. Довгий С. А. Новые технологии в телекоммуникации: выбор технологической архитектуры. Современные тенденции развития / С. А. Довгий, О. В. Копейка, С. П. Поленок. – К.: Укртелеком, 2001. – 281 с.

6. O. Kopeika, I. Tarasenko, A. Kisselevskiy, A. Karichenskiy, T. Valiulin. Softline applies TMF standards as a guide when building Resource Inventory solution for nation-wide carrier Ukraine Telecom // TM Forum Case Study Handbook, Volume 3, May 2007. – P. 27.

7. Разработка стандартов [Електронний ресурс] // – Режим доступу http://www.tiaonline.org/standards/

8. Jew Jonathan. BICSI Data Center Standard: A Resource for Today's Data Center Operators and Designers // BICSI News Magazine, May/June 2010. – 28 p.

9. Niles, Susan. Standardization and Modularity in Data Center Physical Infrastructure // 2011, Schneider Electric. – P. 4.

10. Telecommunications Infrastructure Standard for Data Centers // TIA standard TIA-942. Telecommunications Industry Association. – April 2005. –135 p.

11. ANSI/BICSI 002-2011. Data Center Design and Implementation Best Practices // Committee Approval. – January 2011. – First Published: March 2011. – 367 p.