Microsoft®

Ваше здоровье — наша забота

Информационные системы: ключевые вопросы

Корпорация Microsoft

Часть 3

(Продолжение. Начало в 2005. Т.2 .№1; 2006. Т.3. Вып.4)

Открытые стандарты как средство обеспечения интероперабельности

Под интероперабельностью понимают способность IT-систем обмениваться информацией и совместно ее использовать.

Недавние инициативы в Европе и других регионах демонстрируют возрастание понимания важности интероперабельности в информационном обществе. Широкая интероперабельность информационных технологий дает гражданам возможность использовать разнообразнейший спектр продуктов и услуг благодаря увеличению количества устройств и технологий.

Интероперабельность также имеет большое значение для обмена информацией между системами, создаваемыми разными разработчиками, в медицинских учреждениях и в общественном секторе экономики вообще. Этот обмен может происходить независимо от технологий или платформ, на базе которых построены системы.

Распространение и внедрение открытых стандартов поможет сделать интероперабельными имеющиеся на рынке технологии и программные продукты разных производителей, а затем позволит разнообразным продуктам обмениваться данными и совместно функционировать в сетевой среде.

В соответствии с директивой ЕС относительно программного обеспечения, интероперабельность компонентов компьютерных систем в общем случае означает «способность обмениваться информацией и совместно использовать информацию, которая является предметом обмена».

Ряд известнейших в мире коммуникационных систем с высокой степенью интероперабельности стал успешным именно благодаря способности работать на разных платформах и с разными технологиями, благодаря поддержке стандартизированных форматов данных. Так, применение для форматирования контента Интернет-страниц открытых стандартов, которые базируются на HMTL, XML и родственных им форматах, служит основой высокой интероперабельности разнообразных аппаратных устройств, операционных систем и прикладных программ.

Подобным образом системы передачи SMS-сообщений для мобильных телефонов и других устройств беспроводной связи достигают высокого уровня интероперабельности, благодаря тому, что стандартизированный формат SMS-данных разрешает передавать сообщения при помощи многочисленных конкурирующих платформ для сотовой связи стандартов GSM и 3G.

Сегодня несколько общепринятых открытых интернет-стандартов составляют базу для построения интероперабельных систем. К таким стандартам относятся:

- интернет-стандарты интероперабельности, разработанные консорциумами IETF, W3C и WS-I (например, XML);
- веб-службы как метод обеспечения обмена информацией между разными системами разных разработчиков;
- единый подход к организации метаданных (Дублинское ядро, стандарт RDF);

Средства обеспечения интероперабельности должны опираться на соответствующие открытые стандарты:

- HL7 или Dicom;
- TCP/IP – ведущий протокол транспортного и сетевого уровня;
- протокол передачи гипертекста HTTP и защищенный протокол HTTPS с 128-битовым SSL-шифрованием данных;
- HTML – язык разметки гипертекста, который используется для форматирования веб-страниц;
- XML – язык, который обеспечивает структурированность и однообразие способов представления информации;
- стандарт цифровой подписи от W3C – метод применения цифровых сертификатов для цифрового подписывания информации, которая базируется на использовании открытых стандартов;
- сертификаты x.509, которые применяются, в частности, для создания цифровых сертификатов и цифровой подписи;

• протокол SOAP, который устанавливает правила доступа к системам независимым от производителя способом;
протокол SMTP, предназначенный для обмена сообщениями по электронной почте;
• веб-службы, как первичный независимый от разработчика метод взаимодействия применений через сеть Интернет;
• стандарты консорциума WS-I (WS-Security, WS-Trust, WS-Policy и др.), которые должны обеспечить унифицированность методов защищенного, надежного и прогнозируемого взаимодействия систем.

Внедряя эти средства обеспечения интероперабельности, медицинские учреждения получают возможность обмениваться информацией согласованным способом. Но, кроме этого инструментария общего назначения, нужна, также, специфическая для организации система стандартов, которым должны отвечать упомянутые средства. Такая система создается путем внедрения единой сквозной ИКТ-архитектуры в масштабе организации, которая определяет и, даже, диктует конкретные методы общего использования отдельных средств последовательным и интероперабельным способом.

Возрастающее количество стандартов и спецификаций, связанных с языком XML, демонстрирует преимущества стандартизированных форматов в обеспечении интероперабельности данных, а также разработок разных поставщиков.

Цель среды XML – предоставить исчерпывающий набор открытых и общепринятых стандартов и нормативов, который бы разрешил любой программе, разработанной с учетом этих стандартов, обмениваться данными с другими программами, которые поддерживают формат XML, независимо от языка программирования, на котором они написаны, и платформ, на базе которых они работают.

Медицинским учреждениям важно понимать отличие между открытыми стандартами, которые обеспечивают *интероперабельность применений*, и *программным обеспечением с открытым исходным кодом*. К исходному коду такого программного обеспечения предоставляется свободный доступ, но открытые стандарты оно поддерживает не обязательно.

Целью создания открытых стандартов, как отмечалось, является содействие интероперабельности имеющихся на рынке разнообразных конкурирующих продуктов и услуг путем установления определенного минимального набора требований, которым должны отвечать разработки. Принадлежность того ли иного стандарта к категории «открытых» никак не связана с моделью разработки программного обеспечения, которую применяет разработчик во время внедрения стандарта. Применение открытых стандартов интероперабельности возможно как в коммерческом программном обеспечении, так и в программах с открытым кодом.

Впрочем, последние далеко не всегда отвечают открытым стандартам. Фактически, возможность внесения модификаций в код программного обеспечения, благодаря его общедоступности, создает потенциальный риск нарушения его интероперабельности с устройствами и другими программами.

Итак, нет связи между принадлежностью того или иного программного продукта к программам с открытым кодом, и отдельным и намного более важным вопросом о том, удовлетворяет ли он требованиям открытых стандартов.

Корпорация Microsoft поддерживает открытые стандарты в своих технологиях и продуктах, а также, рациональное повторное использование решений через инициативу «Свободный обмен приложениями и решениями» (Open Application and Solution Sharing – OAS) для правительственных учреждений. Таким образом, корпорация Microsoft оказывает содействие обмену наилучшими практическими решениями, интеллектуальной собственностью и решениями на платформе Microsoft между органами управления, их партнерами, работниками образовательной сферы и разработчиками информационных систем.

На базе инициативы OAS был создан Центр свободного обмена приложениями (OASC), что предлагает:
• веб-платформу, которая открывает доступ к знаниям и решениям;
• объединенная среда, которая обеспечивает общую работу над правительственными решениями, а также их переработку и усовершенствование;
• ряд механизмов для поиска, оценивания и каталогизации решений и проектов;
• открытый форум для партнеров, чтобы они могли презентовать свои решения и возможности.

Центр OASC предоставляет такие преимущества учреждениям, которые работают в области здравоохранения:
• расширение возможностей обмена информацией;
• ускоренная передача информации: можно скорее узнавать, как выполняются решения, и ускорять учебный процесс, связанный с новыми проектами;
• ускорение реализации решений: клиенты могут обмениваться решениями на нашей платформе, которая поможет повысить эффективность работы и предоставит дополнительные преимущества;
• улучшенные возможности повторного использования: можно использовать результаты работы, которую выполнили другие учреждения, сэкономив время и средства и не рискуя потерпеть неудачу (зачем вновь изобретать колесо?!).

Фактически инициатива объединяет большую группу приложений, которые совместно используются во многих органах управления, а также архитектур, документов, исследований, планов и ссылок.

Все материалы и IP-адреса общественным учреждениям и их сотрудникам предоставляются бесплатно. Это еще один пример того, как партнерство с корпорацией Microsoft может помочь повысить качество работы и снизить затраты. В свою очередь, это разрешает органам местного и регионального управления сосредоточить большую часть ограниченных ресурсов на выполнении основных задач, а не на работе вспомогательных служб и обслуживании сложных IKT, которая становится необходимой, если нужно, например, обеспечить совместимость многочисленных технологий разных производителей.

Система метаданных

Эффективный обмен информацией, как внутри медицинских учреждений, так и с другими организациями, требует однозначного толкования терминов, которые используются в многочисленных подразделах органов здравоохранения. Наилучшим способом решения этой задачи есть применение единого языка, каталога и тезауруса метаданных.

Метаданные – это, в сущности, «данные о данных». В этом определении, на первый взгляд несколько тавтологическом, скрыт логический, последовательный подход к эффективному и повторному использованию информации. Например, метаданные музыкальной библиотеки, которая сохраняется на компакт-диске, – это информация, описывающая собственно компакт-диск: название издателя, перечень исполнителей, названия песен и т.п.

Тезаурус является средством, которое может гарантировать, что «сквозная» информация, использующаяся в медицинском учреждении (а также, передаваемая между разными органами

здравоохранения и между медицинскими и другими организациями), является унифицированной, то есть, что одним и тем же метаданным всегда отвечают одни и те же понятия.

Создание каталога стандартных терминов и дескрипторов, его использование в разнообразных службах предусматривает определение общеупотребляемых ключей, которые обеспечивают эффективное получение, и использование информации кем бы то ни было, кто пройдет соответствующую авторизацию.

Разработанная консорциумом W3C технология семантической сети, которая включает в себя среду описания ресурсов (Resource Description Framework, RDF), определяет общую архитектуру метаданных и предназначена для обеспечения совместимости метаданных с помощью общей семантики, структуры и синтаксиса.

Технология семантической сети предусматривает расширение возможностей Интернета благодаря механизмам предоставления информации четко определенного значения, которое разрешает эффективно использовать ее в общей работе, как компьютеров, так и людей.

Инициатива метаданных Дублинского ядра (The Dublin Core Metadata Initiative, DCMI) – общепризнанный открытый форум, посвященный разработке совместных стандартов метаданных на базе инициатив W3C относительно внедрения стандартов RDF и XML.

Концепция метаданных Дублинского ядра дополняет существующие подходы относительно поиска и индексирования сетевых метаданных и используется во многих заинтересованных сообществах, в том числе правительствах, библиотеках, образовательных организациях и коммерческих компаниях.

Система безопасности

Необходимость обеспечения целостности, конфиденциальности и доступности информации в медицинских учреждениях очевидна.

Потребность в защите в равной мере касается как информации, которая помещается во всех информационных системах и передается сетью, так и той, что находится «вне кадра».

Многообразие информации огромно, а ее безопасность должна гарантироваться всегда, ведь каждый день появляются новые сообщения о злоупотреблении и взломах. Вместе с более сложными проблемами, связанными с социотехникой, проблемы защиты информации требуют от ее собственников постоянно быть настороже. Вторжение, атаки, направленные на срыв обслуживания пользователей, незаконное разглашение информации – «постоянные» угрозы, противостоять которым должны тщательно продуманные программы защиты данных. Речь идет, как о внутренних системах и процедурах, так и о тех, которые освещаются в Интернете.

По причинам, обозначенным выше, органы здравоохранения должны придерживаться базовых принципов гарантирования информационной безопасности:

- использование информации в соответствии с законодательством и исключительно с той целью, с которой она предоставляется;
- сведение объемов информации к необходимому минимуму;
- уважение прав граждан или организаций, которых касается использующаяся информация;
- своевременное обновление, обеспечение актуальности и достоверности информации;
- сохранение информации лишь до тех пор, пока она нужна;
- поддержка безопасности информационной среды;
- предоставление информации другим организациям лишь после поступления соответствующих запросов и осуществление защитных мероприятий.

Естественно, что в разных странах в понятие «личная информация» вкладывают разное содержание, которое объясняется отличиями в демократических традициях, балансе прав и обязанностей между гражданами и государством.

В общем случае, личная информация состоит из объективных и субъективных сведений.

Обмен информацией в границах медицинского учреждения, между медицинским учреждением и отдаленными адресатами (другими органами здравоохранения и внешними организациями) должен быть надежно защищен.

Желанию защитить потоки данных противоречит желание применять открытые стандарты интероперабельности, а также открытость сети Интернет, насыщенной узкоспециализированными программными решениями.

Одним из способов достижения баланса между потребностями в безопасности и открытостью является создание защищенной сети только для медицинских учреждений. Такие сети могут использовать преимущества всех стандартов и технологий Интернета (TCP/IP, HTTP, XML и т.п.), вместе с тем, предоставляя доступ и возможность получения услуг закрытому сообществу лиц, которые имеют высокий уровень доверия.

Защищенная сеть медицинского учреждения должна иметь общую «границу» с Интернетом, организованную так, что ее пользователи имеют возможность пользоваться Интернетом, не беспокоясь о защите от вирусов, хакерских атак и др.

Тем не менее, описанный подход связан с потенциальной трудностью: не все внешние заинтересованные организации будут удовлетворять требованиям безопасности или будут иметь пороговую ступень доверия, а значит, они будут лишены информации, в которой нуждаются.

Другим, более гибким, методом является использование Интернета как носителя информации с выделением виртуального сообщества медиков при помощи защищенных ссылок и общей среды аутентификации и авторизации. Таким методом может быть, например, взаимная аутентификация надежных организаций с помощью 128-битового протокола шифрования SSL или технологий VPN.

Ключевым международным стандартом по безопасности информации является, разработанный Международной организацией стандартов (International Standards Organization, ISO), стандарт ISO/IEC 17799:2000 – свод правил и норм по управлению безопасностью в области информационных технологий.

Некоторые органы здравоохранения уже используют этот стандарт во внутренних сетях и требуют от поставщиков его соблюдения. Такое использование может стать моделью и для других медицинских учреждений. Стандарт ISO/IEC 17799:2000 регламентирует такие аспекты:

- планирование последовательности действий;
- контроль над доступом к системе;
- разработка и обслуживание систем;
- физическая защита информации и защита информации в сетях;
- соответствие требованиям;
- защита личной информации;
- защита информации, которая принадлежит организации;
- управление компьютерным обеспечением и сетями;
- классификация IT-активов и контроль над ними;
- политика безопасности.

Еще одним важным стандартом являются, так называемые, *Общие критерии (Common Criteria – CC)* – разработанный при участии правительств, признанный во всем мире стандарт ISO в области оценки защищенности IT-продуктов и систем.

Общие критерии предусматривают сертификацию программных продуктов независимой аккредитованной лабораторией с обязательным придирчивым тестированием и изучением документации. В 2002 году Совет Европы призывал все государства-члены ЕС продвигать Общие критерии и использовать продукты, которые отвечают признанным стандартам.

Корпорация Microsoft на данный момент гарантирует соответствие своих базовых серверных продуктов определенным уровням CC – например, линия продуктов Windows Server аккредитована на уровне EAL4+, а ISA Server – на уровне EAL2.

В органах здравоохранения информационные системы играют все более важную роль. В мире, где большинство дел любой организации ведется в электронном виде, каждый простой или потеря данных имеют ощутимые последствия. Безопасность – это полноценный и жизненно важный компонент предоставления услуг. Общепризнанный набор стандартов и подходов к гарантированию безопасности обеспечивает целостность и доступность данных организаций.

Рекомендации

Корпорация Microsoft рекомендует применять стратегию многоуровневой защиты (Defence in Depth), которая разрешит нашим клиентам удовлетворять собственные требования к безопасности IT-систем. Мы стремимся предоставить технологии, которые дают возможность реализовывать решение по безопасности на всех уровнях, которые будут рассмотрены ниже.

Периметр

Корпорация Microsoft разработала технологию брандмауэра, который защищает, как отдельные рабочие станции, так и корпоративную сеть.

Брандмауэр Windows XP Internet Connection Firewall (ICF) защищает от многих атак (компьютерных вирусов и червей), а также предупреждает отрицательное влияние программ, разработанных злоумышленниками, на компьютер пользователя.

Сервер Internet Security and Acceleration (ISA Server) предоставляет пользователям службы брандмауэра, прокси и вебкеширование.

Брандмауэр выполняет традиционные функции, например фильтрацию портов и протоколов, но, что важнее, он обеспечивает пакетную проверку. Это позволяет проверять данные, введение которых в сеть было разрешено через корректно открытые порты, и предупреждать вторжения червей, вирусов, созданного злоумышленниками кода и других вредных сетевых запросов.

Сеть

Для лучшей защиты сети организации можно использовать функции, встроенные в операционные системы семейства Windows.

IPSec – это открытый стандарт, который расширяет возможности шифрования сетевого протокола TCP/IP, позволяет ставить цифровые подписи и проводить аутентификацию сетевых соединений.

Как беспроводные, так и кабельные сети можно защитить от неавторизованного доступа с помощью стандартизированного промышленного протокола IEEE 802.1X.

Отдаленные клиенты, которые подключаются к веб-приложениям, могут быть защищены с помощью протокола Secure Sockets Layer (SSL), а подключаться к сетям LRG отдаленные пользователи могут, используя протоколы Layer Two Tunnelling (L2TP) и IPSec.

Хост

В усовершенствованных службах конфигурирования семейства Windows Server уменьшено количество служб, которые устанавливаются и активируются по умолчанию, и таким способом уменьшена уязвимая зона системы.

Службы, которые работают под управлением Windows Server, могут выполняться под учетными записями с низким уровнем разрешения, что уменьшает вероятность использования уязвимых мест приложений для получения высокоуровневого доступа к системе. Такие средства автоматического установления обновлений, как Software Update Services и Systems Management Server 2003, снижают затраты на модернизацию систем.

Приложения

Возможности операционных систем Windows, серверных систем Windows (Exchange Server, SQL Server и т.п.) и .NET Framework позволяют разрабатывать безопасные программы.

Приложения могут использовать такие протоколы аутентификации, как Kerberos и SSL Client Certificates, что позволяет защитить пользователей от неавторизованного доступа путем использования встроенных в платформу функций авторизации на базе ролей.

Технологии .NET Framework и ASP.NET дают возможность проверять данные, которые вводятся, и предупреждать введение сознательно искривленных или вредных данных. С их помощью разработчики могут также легко избежать распространенных ошибок, которые могут привести к уязвимости приложений.

Данные

Информация, которая сохраняется на компьютерах пользователей, может быть защищена от неавторизованного доступа с помощью файловой системы с поддержкой шифрования (Windows Encrypting File System), которая шифрует данные в соответствии с промышленным стандартом шифрования 56bit DESX.

Кроме использования криптографических функций, встроенных в операционные системы семейства Windows, технология .NET Framework разрешает разработчикам легко встраивать в приложения такие стандартные криптографические алгоритмы, как RSA, AES и DES.

Возможности резервного копирования и восстановления, которое предоставляют системы Windows Server, разрешают максимизировать время бесперебойной работы системы, оперативно выполнять планы восстановления после перебоев и использовать географически отдаленные датацентры для дублирования ресурсов с целью повышения надежности предоставления услуг.

Библиотека документации по управлению ИКТ-системами и их эксплуатации

Для повышения успешности IT-проектов организации должны создавать библиотеки документации, которая касается широкого круга вопросов по эксплуатации ИКТ-систем и управлению ними. В этой документации обычно описывается метод эффективного проектирования, разработки, развертывания, эксплуатации и поддержки, необходимых для организации IT-решений.

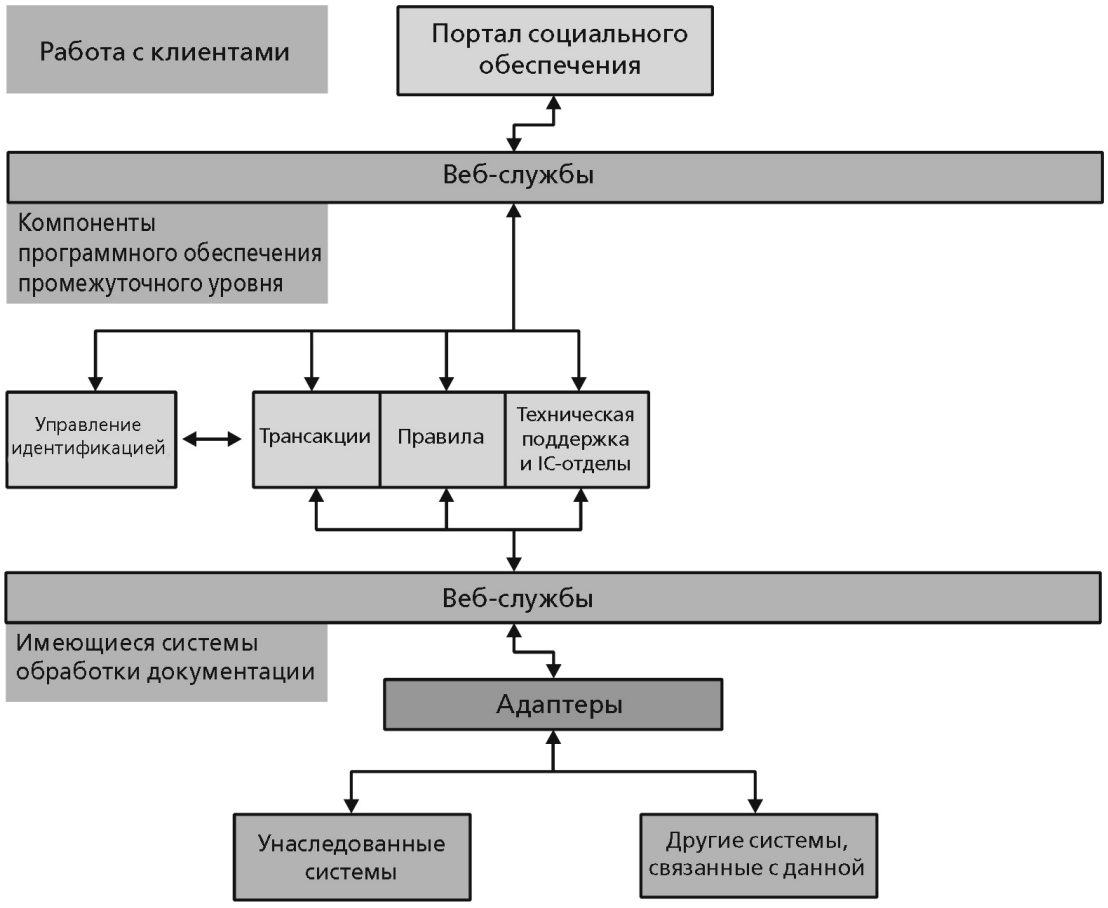
Библиотека по вопросам эксплуатации ИКТ-систем организации и управление ними содержит технические пособия, которые дают возможность организации обеспечить такие критически-важные характеристики ИКТ-решений, как надежность, доступность, возможность поддержки и управляемость, а также решить проблемы, связанные с человеческим фактором, процессами, технологиями и управлением, которые непременно возникают при эксплуатации сложных, распределенных и гетерогенных ИКТ-сред.

Наилучшие промышленные решения в области предоставления ИКТ-услуг были подробно задокументированы в библиотеке ITIL (ICT Infrastructure Library) Управления государственной торговли Великобритании (Office of Government Commerce – OGC). OGC – государственный регулирующий орган, на который возложены функции аккумулирования наилучшего опыта и предоставления рекомендаций по вопросам использования информационных технологий в сфере организации обслуживания. Для этого OGC начинает общие проекты с наибольшими мировыми ИКТ-компаниями, документируя и предоставляя официальный статус опыту, накопленному в данной области.

Библиотека ITIL в данный момент состоит из более 40 томов, каждый из которых посвящен определенной функции управления IT-службами и содержит ссылки на все друг тома.

Медицинские учреждения могут использовать библиотеку ITIL для того, чтобы соединить общепризнанные промышленные стандарты в области ИКТ-технологий с конкретными рекомендациями относительно использования продуктов и технологий, развернутых в их IT-средах.

Корпорацией Microsoft разработана также собственная техническая библиотека (Microsoft Operations Framework – MOF), которая базируется на библиотеке ITIL и расширяет ее. MOF содержит рекомендации относительно поддержки распределенных ИКТ-сред и отраслевых тенденций, например, таких как хостинг приложения и системы электронной коммерции на базе веб-трансакций.



Использование стандартов интероперабельности в интегрированных информационных системах.

Совместные межорганизационные IT-архитектуры

В области здравоохранения разработка любых информационных систем и инвестирование в них может происходить в контексте четко определенной IT-архитектури масштаба организации, которая направлена на создание эффективной сервисно-ориентированной среды. Оптимальным путем создания такой среды является:

- использование согласованных интерфейсов (схем, методов и др.);
- применение согласованных стандартов обмена информацией (например, веб-служб);
- разработка IT-архитектур отдельных организаций в контексте межорганизационной сервисно-ориентированной архитектуры (SOA) всей системы здравоохранения.

Открытые стандарты совместимости разрешают связывать разнообразные источники информации в единую систему информационных услуг.

Результатом тщательно разработанной IT-стратегии станет реализация «шины сообщений», основы всей SOA организации. Службы, соединенные с этой шиной, могут базироваться на разных технологических платформах, но поскольку они будут отвечать открытым стандартам совместимости, сообщение между ними будут пересылаться свободно. Это происходит благодаря тому, что «шина сообщений», в свою очередь, базируется на ключевых стандартах (например, совместимости данных), которые разрешают осуществлять надежный и согласованный обмен информацией между системами.

Принятие этой модели будет иметь положительное влияние на процесс обмена информацией, как между органами здравоохранения, так и между медицинскими учреждениями и посторонними организациями.

Все больше стран переходит на такие открытые стандарты интероперабельности, как XML и SOAP/веб-службы, чтобы обеспечить интероперабельность в границах имеющихся систем и между ними. Одни и те же стандарты разрешат упростить процедуру обмена информацией между медицинскими учреждениями и другими организациями.

Как видно из изображенной на рисунке модели, веб-службы сыграют ключевую роль в развитии SOA, поскольку разрешают организациям создавать нежестко связанную ИКТ-инфраструктуру.

Такие стандарты веб-служб, как XML, UDDI и SOAP дают возможность осуществлять коммуникации в сети в том формате, в котором это необходимо. Создание на базе этих стандартов бизнес-процессов, к которым можно будет предоставлять доступ через веб-службы, разрешит сделать ИКТ более соответствующим потребностям организаций, которые постоянно меняются.

Корпорация Microsoft предоставляет платформу для развертывания интегрированных инновационных решений на базе таких открытых стандартов, как XML, UDDI, SOAP и связанных с ними технологий открытых стандартов, обеспечивая интероперабельность своей продукции, благодаря передовым достижениям всемирного масштаба.

Литература

1. Runciman W. B., Roughead E. E., Semple S. J., Adams R. J. Adverse drug events and medication errors in Australia. Int J Qual Health Care. 2003 Dec; 15 Suppl 1:i49–59.
2. M. Pirmohamed, S. James, S. Meakin, C. Green, A. K. Scott, T. J. Walley, K. Farrar, B. K. Park, A. M. Breckenridge. Adverse drug reactions as cause of admission to hospital: prospective analysis of 18 820 patients BMJ. 2004 July 3; 329 (7456): 1519.
3. Rome R. M., Fortune D. W. The role of second-look laparotomy in the management of patients with ovarian carcinoma. Aust N Z J Obstet Gynaecol. 1988 Nov;28(4):318–23.
4. Johnson M. A., Davis P., McEwan A. J., Jhangri G. S., Warshawski R., Gargum A., Ethier J., Anderson W. W. Preliminary findings from a teleultrasound study in Alberta. Telemed J. 1998 Fall; 4(3):267–76.
5. Rogo K. O., Ojwang S. B., Stendahl U. Second look laparotomy — its role in the management of ovarian carcinoma. East Afr Med J. 1989 Dec; 66(12): 844–50. Review.
6. Устный доклад на Конгрессе по вопросам услуг e-Health в 2003 г.: Meer A., Weber A. Use of computer assisted telephone triage in out of hours primary care and the ISPM study: Niemann S., Meer A., Simonin C., Abel T. Medical telephone triage and subsequent patient behaviour: How do they compare? Swiss Med Wkly 2004; 134:126–131.
7. Lattimer V., George S., Thompson F., Thomas E., Mullee M., Turnbull J., et al. Safety and effectiveness of nurse telephone consultation in out of hours primary care: randomised controlled trial. The South Wiltshire Out of Hours Project (SWOOP) Group. Br Med J 1998; 317:1054–9.
8. Forbis, S. «Designing educational computer games.» Health Educ. 14.6 (1983): 15–18.
9. Brown, S. J. et al. «Educational video game for juvenile diabetes: results of a controlled trial.» Med.Inform. (Lond) 22.1 (1997): 77–89. Lehmann, E. D. «Interactive educational simulators in diabetes care.» Med.Inform. (Lond) 22.1 (1997): 47–76.
10. Turnin, M. C. et al. «Evaluation of microcomputer nutritional teaching games in 1,876 children at school.» Diabetes Metab 27.4 Pt 1 (2001): 459–64. Yawn, B. P. et al. «An in-school CD-ROM asthma education program.» J.Sch Health 70.4 (2000): 153–59.
11. Bosworth, K. et al. «Using multimedia to teach conflict-resolution skills to young adolescents.» Am.J.Prev.Med. 12.5 Suppl. (1996): 65–74.

Переписка

Майкрософт Украина
а/я 166, Киев, 04070, Украина
тел.: +380 44 496 0310
факс: +380 44 496 0317
http://www.microsoft.com/ukraine