ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ И НАУЧНОЙ РАБОТЕ

Сборник материалов Всероссийской научно-практической конференции с международным участием

Часть 1

Йошкар-Ола
Марийский государственный технический университет
2009

УДК 004:371.1
ББК 74.5ся43
И 74

И 74 **Информационные технологии в профессиональной деятельности и научной работе:** сборник материалов Всероссийской научно-практической конференции с международным участием. – Йошкар-Ола: Марийский государственный технический университет: в 2 ч. – Ч.1. – 2009.– 160 с.

ISBN 978-5-8158-0694-8

В настоящий сборник включены статьи и краткие сообщения по материалам Всероссийской научно-практической конференции с международным участием по результатам исследований в следующих областях: базы знаний и интеллектуальные системы; системы классификации и распознавания образов; сетевые технологии и коммуникации; специальные системы, а также разработки средств компьютерного обучения, инновационного образования и дистанционного тестирования.

УДК 004:371.1
ББК 74.5ся43

ISBN 978-5-8158-0694-8

УДК 004.732

Д.В. Дюгуров
г. Ижевск, Удмуртский государственный университет

ОТКРЫТЫЕ СЕТИ ПРОТИВ «ЧЕРНОГО ЯЩИКА»

Создание и рациональное использование общих вычислительных ресурсов является одной из важнейших задач информатизации в целом. Возможность масштабирования сетей, интеграции между собой уже созданных сегментов напрямую зависит от выбранных сетевых платформ. Особую актуальность эта проблема приобретает в профильных вузах. В данном случае учебному заведению необходимо решать сразу несколько задач:

- подготовка специалистов (программистов, системотехников, специалистов по безопасности информации и пр.), зачастую в отрыве от реальных производств;
- поиск источников финансирования;
- соответствие технической базы требованиям времени;
- обеспечение функционирования и развития IT отрасли в регионе.

Для этого учебное заведение должно обладать высококлассными специалистами из числа профессорско-преподавательского состава, «рабочей силой» - студентами и средствами разработки. Одним из таких инструментов должна быть распределенная сеть, состоящая из мощных вычислительных машин, адекватных им операционных систем и сред разработки. Использование такого комплекса позволит учебному заведению получать заказы, выполнять реальные проекты и погружать студентов в производственную среду без ущерба для учебного процесса с огромной практической пользой. Следует отметить, что в настоящее время при реализации подобных корпоративных сетей используется принцип «черного ящика» - никому из пользователей неизвестно ничего об инфраструктуре сети, эта информация является неотъемлемой частью политики безопасности.

В качестве решения перечисленных задач предлагается проект вычислительной сети на базе имеющихся в распоряжении факультета информационных технологий и вычислительной техники Удмуртского государственного университета (УдГУ) компьютеров, серверных операционных систем Microsoft Windows Server 2003 SP2, клиентских операционных систем Windows XP Professional SP 3 и лицензионных средств разработки, распространяемых для высших учебных заведений. Мас-

штабы данной сети сопоставимы с сетью крупного промышленного предприятия. Следует также отметить, что использование студентами лицензионного программного обеспечения, установленного на факультетских серверах, позволяет повысить культуру будущих специалистов и сократить количество ошибок в их продуктах.

Наличие данного инструмента должно породить особое содружество студентов: инициативные студенты, получая определенные заказы, могут формировать собственные команды, используя факультетскую сеть в качестве средства разработки. Образовав собственные компании после окончания вуза, они могут продолжать использовать университетскую сеть и ее ресурсы. В результате вокруг университета образуется бизнес-окружение, которое будет потреблять выпускников соответствующих специальностей и снабжать студентов практической работой, что является идеальным вариантом для вуза и высшего образования в целом. Это позволяет университету участвовать в выгодных коммерческих проектах и повышает престиж преподавательской деятельности среди бывших студентов, что обеспечит воспроизводство кадров для университета за счет привлечения этих специалистов в учебный процесс.

Описанную выше сеть далее назовем *вычислительной сетью с открытой инфраструктурой*. Причем «открытость» состоит в том, что студенты, обучающиеся или обучавшиеся в университете, могут использовать сетевые ресурсы для решения любых прикладных задач, им известно, как организована сеть, какие используются программные продукты и аппаратные средства. Вместе с тем часть данной сети непосредственно используется в учебном процессе как техническое средство обучения.

Существенным обстоятельством здесь является то, что «открытость» не является угрозой безопасности сети в целом. Безопасность такой сети заключается не в сокрытии информации о ее логической и физической инфраструктурах, а разделении уровней административного вмешательства пользователей в систему на основе «принципа наименьших привилегий».

Смысл принципа наименьших привилегий в следующем – каждому пользователю должен быть явно разрешен доступ только к тем ресурсам системы, которые необходимы ему для выполнения своих обязанностей или удовлетворении потребностей в рамках утвержденного бизнес-процесса.

Открыв информацию и сетевой инфраструктуре широкому кругу пользователей, наряду с разделением ролей мы оставляем еще один элемент сетевой безопасности – учетные данные участников безопасно-

сти (логины и пароли). На этапе первоначального функционирования вычислительной сети с открытой инфраструктурой ее безопасность обеспечивают встроенные стойкие алгоритмы аутентификации. В дальнейшем в систему безопасности можно вносить коррективы, используя предложения пользователей сети, обнаруживших в ней «узкие места». В этом механизме учтена и психологическая сторона вопроса, – никому из пользователей не захочется сознательно портить или оставлять уязвимым инструмент, который он использует в работе.

Итак, нам необходим инструмент, с помощью которого можно:

- управлять разрозненной массой общих ресурсов;
- по возможности совместно использовать вычислительные мощности;
- следить за потоками информации внутри организации;
- обеспечивать безопасное хранение и использование информации;
- функционирование такого инструмента должно быть четко задокументировано и понятно знакомящемуся с документами.

Для достижения этой цели необходимо:

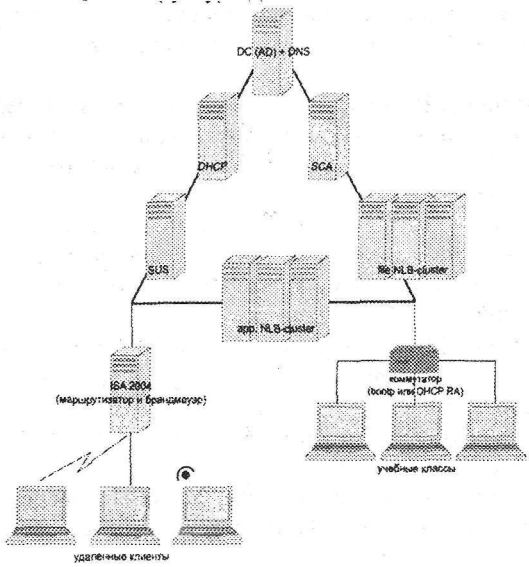
- собственно компьютеры, объединенные в сеть по определенным правилам;
- защищенная база данных, включающая в себя всю информацию об общих объектах (упрощает поиск), пользователях, компьютерах (упрощает администрирование);
- инструменты управления этой базой данных;
- инструменты отказоустойчивости этой базы данных;
- инструменты восстановления этой базы и ее частей.

Все поставленные задачи можно решить, воспользовавшись возможностями доменной сетевой структуры с Активным каталогом (Active Directory), реплики которого находятся в узлах маршрутизации. Отказоустойчивость подобной системы можно обеспечить с помощью репликации нужных частей каталога между несколькими контроллерами домена по протоколу LDAP.

Предполагается, что корневым является домен второго уровня **fitvt.ru**, а поддомены **adm.fitvt.ru**, **st.fitvt.ru**, **test.fitvt.ru** – это административная, учебная и тестовая подсети соответственно. Однозначное соответствие элементов физической и логической инфраструктур сети в дальнейшем изложении позволяет использовать термины «подсеть» и «поддомен» как синонимы.

Внутренняя структура каждого из поддоменов состоит из одинаковых базовых элементов. При необходимости в каждом из поддоменов

размещаются сервера со специфическими ролями. Общие части структуры поддоменов мы рассматриваются на примере **st.fitvt.ru**, Схема поддомена **st.fitvt.ru** представлена на рисунке.



Структура домена st.fitvt.ru

Обслуживать данную сеть должна специальная служба старшего системного администратора. Причем функции участников этой группы должны быть разделены не только по направленности (решение проблем с адресацией отдельно от восстановление системы после сбоя и др.), но и по уровню административного вмешательства (в пределах всего домена, в пределах поддоменов, на рябее серверов и т.д.).

Информацию о структуре юнитов в доменах, групповых политиках, свойствах профилей пользователей, механизмах идентификации и аутентификации, стратегии архивирования, квотирования дискового пространства и прочих элементах инфраструктуры открытых сетей можно найти в работах автора из библиографического списка.

Библиографический список

1. Дюгуров Д.В. Внедрение вычислительной сети с открытой инфраструктурой в образовательный процесс // Тр. 14 всероссийской научно-методической конференции «Телематика 2007» / – СПб., 2007, Т.2. – С. 297.

2. Дюгуров Д.В. Управление факультетом и модернизация учебного процесса с помощью вычислительной сети с открытой инфраструктурой. / Тр. 35 итоговой студ. научной конференции / Удмуртский гос. университет. – Ижевск, – С. 39 – 40.

3. Дюгуров Д.В. Сети с открытой инфраструктурой: безопасный инструмент обучения и производства // Сборник докладов 6 международной научно-методической конференции «НОТВ». – Екатеринбург, УГТУ-УПИ, 2008. – С. 27 – 32.

4. Дюгуров Д.В. К вопросу о безопасности сетей с открытой инфраструктурой //Тр. 15 всероссийской научно-методической конференции «Телематика 2008» – СПб, 2008. – С. 310.

5. Дюгуров Д.В. Концепция информатизации УдГУ. // Дистанционное обучение – М., 2008, №5.

6. Дюгуров Д.В. Принципы построения университетской сети с открытой инфраструктурой // Научно-технические ведомости СПбГПУ, 2009. №6(69) – С. 64 – 68.

7. Дюгуров Д.В. Сети с открытой инфраструктурой: концепция проекта на базе факультетат ИТИВТ Удмуртского государственного университета // Труды международной конференции «Перспективы развития телекоммуникациооных систем и информационные технологии» – СПб, Политехнический институт, – 2008, – С. 446 – 457.