Известия Гомельского государственного университета
имени Ф. Скорины, № 6(69), 2011

УДК 004.5

Программно-информационное обеспечение системы авторизации доступа к источникам научно-технической и деловой информации ДОСТУП

А. И. Кучеров, Е. А. Левчук

В статье рассмотрены структура и функции комплекса для авторизации доступа к источникам научной, технической и промышленной информации. Предложенные средства позволяют улучшить управление сетевым доменом.
Ключевые слова: авторизация доступа, сетевой домен, система ДОСТУП.

The structure and functions of the complex for an access authorization to sources of scientific, technical and business information are considered in the article. The means offered allow to improve the management of a network domain.
Keywords: access authorization, network domain, ACCESS system.

Введение

Программно-информационное обеспечение системы авторизации доступа к источникам научно-технической и деловой информации ДОСТУП представляет собой совокупность общесистемных и специализированных программно-информационных средств. Информационное обеспечение данной системы базируется на современных информационных технологиях.

При развертывании системы ДОСТУП целесообразно использовать:

– пользовательскую операционную систему Microsoft Windows 2000 Professional SP4 или более новую (Windows XP Professional, Windows Vista, Windows 7);

– серверную операционную систему Microsoft Windows 2008 Server;

– язык программирования VBScript;

– системные утилиты от фирмы Microsoft;

– операционная система для разработки может быть любая из выше перечисленных.

Комплекс технических средств системы ДОСТУП обеспечивает гарантированные надежные условия обработки и хранения данных. Для этого серверная станция снабжена надежной дисковой подсистемой RAID уровня 0 с зеркальным копированием данных, обеспечивающей защиту от сбоев дисковых накопителей. Для обеспечения резервного копирования данных система снабжена аппаратными средствами, соответствующими выбранной стратегии резервного копирования. Все рабочие станции оснащены сетевыми адаптерами со скоростью передачи не ниже 100 Мбит/с и интегрированы в локальную сеть.

Система ДОСТУП предполагает наличие следующих технических компонентов:

– файловый сервер на базе процессора с тактовой частотой от 1 ГГц, оперативной памятью не менее 2 Гбайт и дисковым пространством (RAID) от 200 Гбайт для накопления и хранения информации (файловый-сервер может совмещать в себе и функции принт-сервера);

– контроллер домена – сервер на базе процессора с тактовой частотой от 2 ГГц, оперативной памятью не менее 2 Гбайт и дисковым пространством (RAID) от 200 Гбайт и выше для накопления и хранения информации;

– устройства бесперебойного питания мощностью от 1000W;

– рабочие станции на базе процессора с тактовой частотой от 1 ГГц, оперативной памятью не менее 1 Гбайт и дисковым пространством от 30 Гбайт и выше для накопления и хранения информации.

Порядок функционирования системы ДОСТУП определяется эксплуатационной документацией на систему. Структура и функции обслуживающего персонала, обеспечивающего эксплуатацию системы, должны быть определены в штатном расписании, должностных инструкциях и в документации на систему.

Потоки данных в системе

Основные потоки данных в системе ДОСТУП порождаются следующими видами информации:

– первичная информация, вводимая в БД Active Directory;

– вторичная информация, вводимая в БД Active Directory автоматизировано из вспомогательного текстового файла при помощи скриптов Visual Basic;

– модификация, удаление устаревшей информации;

– поисковые запросы в БД Active Directory;

– результаты поиска по запросам.

В этом случае под всеми видами информации необходимо понимать различные данные о пользователях и компьютерах, принадлежащих корпоративной сети.

Первичная информация о пользователях корпоративной сети формируется из приказов и распоряжений по организации, использующей систему. Каждый пользователь корпоративной сети обладает определенными правами на использование вычислительных ресурсов сети. Пользователи с аналогичными правами объединяются в группы пользователей. Каждому пользователю предоставляется личная папка на сервере для хранения информации, доступная теоретически только ему. Также в корпоративной сети имеется множество других различных ресурсов, доступных некоторым пользователям или группам пользователей. Все эти ресурсы предоставляются согласно должностным инструкциям и другим распоряжениям.

Первичная информация о компьютерах, входящих в корпоративную сеть, формируется из: технических характеристик вычислительной техники; имени компьютера, определяемого исходя из места его расположения (например, К5-4-1 – корпус 5, аудитория 4-1); MAC-адреса сетевой карты, установленной на компьютере, и другой информации.

Внесением первичной информации в БД Active Directory локально занимается администратор сети.

Вторичная информация хранится во вспомогательном текстовом файле, который формирует администратор корпоративной сети исходя также из приказов и распоряжений по организации. В этом тестовом файле хранится информация о том, какой пользователь принадлежит к какой группе пользователей, также хранится информация о временной блокировке пользователей.

Внесением вторичной информации в БД Active Directory занимаются подпрограммы в виде скриптов Visual Basic, которые запускает администратор сети. При помощи этих скриптов также создаются личные директории на сервере с соответствующими правами на доступ к ним.

Модернизация и удаление устаревшей информации осуществляется как вручную, так и с использованием автоматизации – скриптами Visual Basic. Данные для автоматизации берутся из текстового файла.

Поисковые запросы к БД Active Directory могут формировать как пользователи корпоративной сети, так и администратор сети. Только у пользователей права очень ограничены. Результаты поисковых запросов можно выводить как на экран монитора, так и на принтер.

Диагностированием автоматизированной системы занимается администратор корпоративной сети, используя ОС, установленную на сервере.

Сроки и порядок комплектования штатов и обучения персонала определяется руководством организации, использующей систему ДОСТУП. В общем случае для обеспечения функционирования системы достаточно администратора корпоративной сети и его заместителей, если такие предусмотрены штатным расписанием организации.

Системой реализуются следующие задачи:

– ввод первичной информации в БД Active Directory;

– модификация, удаление устаревшей информации;

– ввод вторичной информации;

– репликация БД Active Directory;

– поисковые запросы в БД Active Directory;

– вывод результатов поиска по запросам;
– создание личных папок пользователей корпоративной сети;
– разграничение прав доступа к ресурсам корпоративной сети;
– ведение аудита входа и выхода на рабочей станции;
– ведение аудита использования сетевых ресурсов;
– автоматизация ввода вторичной информации;
– автоматизация модификации и удаления устаревшей информации.

Решения по составу программных средств, языкам деятельности, алгоритмам процедур и операций и методам их реализации

Современным оптимальным решением для развертывания системы ДОСТУП послужит ОС Windows 2008 Server. Так как она в своем составе имеет Active Directory, которая служит базой данных для хранения информации о пользователях, компьютерах и предоставленных сетевых ресурсах корпоративной сети. Установить и настроить ОС можно достаточно быстро, это зависит от квалификации администратора сети. Выбранная ОС обладает большим количеством сервисов, в частности: защитой от несанкционированного доступа, шифрованием данных, резервным копированием данных, надежностью и др. Эта ОС поддерживает большое количество языков программирования. Для автоматизации настройки и управления сервисами используются два скриптовых языка программирования Visual Basic Script и Java Script.

Для написания системы автоматизации ДОСТУП использовался скриптовый язык программирования Visual Basic Script.

Подготовка к работе

Система ДОСТУП может разместиться на любом современном носителе информации, будь то гибкий магнитный диск, CD-диск, DVD-диск, Flash-диск и др. Файлы размещены в каталоге под именем *AdminScripts*. Дерево файлов и каталогов изображено ниже.

```
\---AdminScripts
    |   reset_home_drive.vbs
    |   UserDir.vbs
    |   Group1.txt
    |   Group2.txt
    |
    \---UserManager
        |   ManageGroup1.bat
        |   ManageGroup2.bat
        |   UserFolderManager.vbs
        |
        \---AddModifyRights
                AddModifyRights.exe
                SecurityUtils.pas
```

Этот каталог необходимо разместить на одном из дисков сервера, например на диске *C*.

Файл *reset_home_drive.vbs* является текстовым и исполняемым, создан на основе VB Script. Он предназначен для установки параметров пользователя: HomeDrive, HomeDirectory. В этом файле также настраивается имя контроллера домена и объектные модули.

Файл *UserDir.vbs* является текстовым и исполняемым, создан на основе VB Script. Он предназначен для связывания личной папки «Мои документы» с сетевым диском на сервере. В свою очередь, на сервере имеется личная папка, представленная как сетевой диск. Эта папка создается другим скриптом.

Файлы *Group1.txt* и *Group2.txt* являются текстовыми и предназначены для хранения имен пользователей, которые должны входить в группы Group1 и Group2 соответственно. Таких файлов должно быть столько, сколько и групп пользователей на сервере.

Файл *UserFolderManager.vbs* является текстовым и исполняемым, создан на основе VB Script. Он является основным компонентом системы ДОСТУП. Этот модуль создает директории для вновь зарегистрированных пользователей и также разграничивает права доступа на них. Еще одной из функций этого модуля является удаление неиспользуемых директорий, то есть директорий тех пользователей, чьи учетные записи отсутствуют на сервере – контроллере домена. В этом файле также настраивается имя контроллера домена и объектные модули.

Файлы *ManageGroup1.bat* и *ManageGroup2.bat* являются текстовыми и исполняемыми, предназначены для активизации основного модуля *UserFolderManager.vbs*. Каждый из этих файлов использует функции основного модуля *UserFolderManager.vbs,* но для определенной группы.

Файл AddModifyRights.exe является исполняемым модулем. Он является вспомогательным по отношению к основному модулю *UserFolderManager.vbs*. Другие файлы – это исходные файлы для AddModifyRights.exe, созданные на языке программирования Object Pascal.

В файлах *reset_home_drive.vbs, UserFolderManager.vbs* необходимо произвести настройки и указать:

– действительное полное имя контроллера домена (MATH-SERVER заменить на свое);

– имя домена (MATH заменить на свое);

– полное имя домена (math.gsu.unibel.by заменить на свое);

– OU – object unit (объектный модуль), из которого следует брать пользователей и другие параметры, изменять исходя из настроек вашего сервера.

Эксплуатация системы

Первым шагом администратора будет создание необходимого количества файлов, в которых будут храниться сетевые имена пользователей по группам принадлежности, например *Group1.txt*, *Group2.txt* и т.д. Имена файлов желательно указывать соответственно именам групп на сервере.

На следующем шаге следует изменить файлы *ManageGroup1.bat, ManageGroup2.bat*, а при необходимости создать аналогичные файлы и для других групп. В этих файлах изменить строку следующего вида: *userfoldermanager.vbs c:\AdminScripts\Group1.txt d:\Groups Users -r –o*. В этой строке прописываются пути к директории с программной системой, а также указывается имя файла, содержащего пользователей определенной группы.

На предпоследнем шаге администратору необходимо заполнить текстовые файлы именами пользователей сети.

Для запуска программного комплекса на выполнение необходимо вызывать исполняемые файлы с расширением *bat* из вложенной директории *UserManager* в директории *AdminScripts*, которая должна размещаться на одном из разделов жесткого диска. Имя файла для запуска программного комплекса, например *ManageGroup1.bat.*

По окончании работы системы ДОСТУП на сервере в указанном месте будут созданы личные папки пользователей с соответствующими правами доступа, а сетевые имена пользователей помещены в заданные группы пользователей.

Заключение

Таким образом, действия администратора корпоративной сети можно описать четырьмя этапами:

1 этап – Установка операционной системы Windows 2008 Server или более новой на сервер. Она может устанавливаться на файл-сервер, контроллер домена, web-сервер и т.д.

2 этап – Настройка Active Directory (настройка групповых политик, разграничение

прав доступа, создание учетных записей пользователей, создание групп пользователей в соответствии с приложением А).

3 этап – Разделение пользователей на группы.

4 этап – Создание личных папок на сервере.

1-й и 2-й этапы администратор сети выполняет в соответствии с руководством по эксплуатации операционной системы Windows 2008 Server или более новой версии. Администратор корпоративной сети перед эксплуатацией системы ДОСТУП должен на сервере – контролере домена установить операционную систему Windows 2008 Server или более новую, а также установить и настроить систему Active Directory (этапы 1 и 2). 3-й и 4-й этапы выполняются администратором с помощью созданной системы ДОСТУП в полностью автоматизированном режиме.

Гомельский государственный
университет им. Ф. Скорины

Поступило 01.11.11