УДК- 681.3:06

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ ДИСТАНЦИОННОГО ОБУЧЕНИЯ КГУСТА ИМ. Н.ИСАНОВА

Ю.В.ШТЕТИН, С.А.КУЗЬМЕНКО
E.mail. ksucta@elcat.kg

Макалада Н. Исанов атындагы КМКТАУнун дистанттык билим берүү системасынын берилиш базасындагы маалыматты эффективдүү коргоо боюнча чаралардын комплекси каралат.

В статье рассматривается комплекс мер по эффективной защите информации в базе данных системы дистанционного образования КГУСТА им. Н.Исанова.

In article the package of measures on effective protection of information in a database of system of remote education KSUCTA of N. Isanov is considered.

Сегодня Интернет прочно вошел в нашу жизнь. Современное образование немыслимо без компьютеров и Интернета. Большинство современных школьников и студентов активно используют компьютер и Интернет в своей жизни и образовании.

В современном обществе при бурном информационном росте специалисту требуется учиться практически всю жизнь. Раньше можно было позволить себе обучиться один раз и навсегда. Этого запаса знаний хватало на всю жизнь. Сегодня идея "образования через всю жизнь" приводит к необходимости поиска новых методов передачи знаний и технологий обучения.

Использование Интернет-технологий и дистанционного обучения открывает новые возможности для непрерывного обучения специалистов и переучивания специалистов, получения второго образования, делает обучение более доступным.

В то же время необходимость получения основного образования в течение всей жизни или переквалификации развивают потенциал дистанционного обучения. С развитием и распространением Интернет-технологий у дистанционного обучения появились новые возможности. В мире появилось огромное количество курсов дистанционного обучения и целые университеты дистанционного обучения /1/.

Наш университет не стал исключением и одним из первых вузов в Кыргызстане начал внедрение системы дистанционного обучения в структуру университета. Первым шагом в этом непростом процессе внедрения стало приобретение лицензионного программного обеспечения. При долгом мониторинге рынка систем дистанционного обучения выбор остановился на программе российских разработчиков СДО «Прометей» компании ООО «Виртуальные технологии в образовании».

С помощью Системы дистанционного обучения (СДО) «Прометей» можно построить в Интернет или Интранет виртуальный университет и проводить дистанционное обучение большого числа слушателей-студентов, автоматизировав при этом весь учебный цикл – от приема заявок до отметки о выдаче итогового сертификата. СДО "Прометей" эффективно используется в различных проектах, государственных и корпоративных структурах, ведущими учебными заведениями России, Украины, Казахстана, Беларуси и других стран СНГ.

Модуль «Учебный портал» позволяет использовать СДО «Прометей» в качестве комплексной системы управления обучением и контентом. Благодаря функциям ведения лент новостей и редактирования информационных блоков этим порталом может управлять рядовой пользователь компьютера.

К серверу СДО «Прометей» и клиентским компьютерам предъявляются различные системные требования.

Сервер СДО «Прометей» – программный комплекс, обеспечивающий предоставление удаленного доступа к объектам СДО и ведение базы данных учебного комплекса. Сервер работает на независимой компьютерной системе, подключенной к Интернету, корпоративной или локальной сети.

Клиентским называется компьютер, с которого участники учебного процесса (администраторы, организаторы, тьюторы и слушатели) получают доступ к функциям системы, то есть взаимодействуют с учебным комплексом «Прометей».

Как и любая система, содержащая конфиденциальную информацию, хранящуюся в базе данных (БД), она должна иметь достойную защиту от всякого рода несанкционированных проникновений.

А) Система безопасности СДО «Прометей» построена следующим образом:

1. При создании слушателя создается логин в ActiveDirectory и заносится в группы SDO, SDOStudents.
2. При создании персонала создается логин в ActiveDirectory и заносится в группы SDO, SDOStaff. Если пользователь – администратор СДО «Прометей», то его логин заносится также в группу SDOAdmins.
3. При создании книги в ActiveDirectory появляется соответствующая локальная группа SDOBooks_{…}.
4. При создании учебной группы в ActiveDirectory появляется соответствующая глобальная группа SDOStudentsG{…}.
5. Если слушатель учится в учебной группе, то его логин занесен в соответствующую учебной группе глобальную группу в ActiveDirectory.
6. Если учебная группа учится по какому-либо курсу и этому курсу соответствует какая-либо книга, то глобальная группа в ActiveDirectory, соответствующая учебной группе, заносится в локальную группу в ActiveDirectory, соответствующую книге.

Б) NTFS-разрешения на папки сайта для групп СДО «Прометей»

1. /close/ - SDO - read
2. /close/staff/ - SDOStaff-read
3. /close/students/ - SDOStudents-read
4. /close/staff/admin/ - SDOAdmins-read
5. папка /close/store/. В этой папке хранится информация, накапливающаяся по мере использования СДО «Прометей».
6. /close/store/books. В этой папке находятся учебные материалы. Разрешения: SDOStaff – read, SDOAdmins – modify. Учебные материалы копируются в эту папку и находятся в директориях с именем, соответствующем GUID'у книги (Primary key таблицы Books). При создании книги, т.е. при создании директории, соответствующей книге в /close/store/books/, на нее автоматически ставится разрешение read для соответствующей локальной группы в AD (SDOBook_{…}). Таким образом, если логин слушателя не входит в глобальную группу, соответствующую учебной группе (SDOStudentG_{…}), которая учится по курсу, по которому книга, то слушателю будет отказано в доступе на просмотр материалов книги, даже если он введет прямой URL.
7. Остальные папки в /close/store/ наследуют NTFS-разрешения /close/store/.

При таком построении защиты системы безопасности СДО «Прометей», возникает дополнительная необходимость в обеспечении безопасности Active Directory.

Active Directory – это служба каталога (directory service), реализованная компанией Microsoft. В свою очередь, служба каталога – это централизованное хранилище информации обо всех ресурсах предприятия или учебного заведения, таких как компьютеры, пользователи, группы, приложения, общие папки, принтеры и другие объекты. Не следует думать, что служба каталога позволяет хранить информацию только о том, что относится к компьютерам. За счет возможности добавлять новые классы

объектов каталог может хранить информацию о любых ресурсах, например, таких, как столы, кофеварки, проекторы и т.д. Основной административной единицей Active Directory является домен (domain). Однако предприятие может включать в свой каталог Active Directory более одного домена. Когда несколько доменов объединяются родительско-дочерними доверительными отношениями и совместно используют общее непрерывное пространство имен DNS, они образуют логические структуры, называемые деревьями (trees). При проектировании структуры доменов Active Directory следует учитывать следующие моменты, напрямую влияющие на безопасность. Во-первых, границами домена ограничены права административных пользователей. Это значит, что администратор своего домена является обычным непривилегированным пользователем в другом домене. Во-вторых, некоторые настройки безопасности, например, минимальная длина пароля, могут контролироваться только на уровне домена, но не ниже. Это означает, что невозможно сделать разную минимальную длину пароля для разных пользователей одного домена, а если это все-таки требуется, то необходимо создавать два или более домена. Домен создается в тот момент, когда какому-либо компьютеру в сети администратор назначает роль контроллера домена (domain controller). Клиентские компьютеры работают со службой каталога (точнее, с контроллером домена) по протоколу LDAP – стандартному протоколу для работы с каталогом.

Основные возможности Active Directory в сфере безопасности

В Active Directory можно выделить несколько возможностей, непосредственно относящихся к информационной безопасности, которые будут обсуждаться далее. Возможность создания древовидной структуры внутри домена с помощью подразделений (organization units, OU). Подразделения представляют собой контейнеры внутри домена, позволяющие группировать объекты для удобства администрирования или для последующей автоматизированной настройки этих объектов с помощью групповой политики (Group policy). Если провести аналогию с файловой системой, то подразделение можно сравнить с папкой. Внутри подразделения могут находиться различные объекты Active Directory: учетные записи пользователей (users), учетные записи компьютеров (computers), группы (groups), опубликованные общие папки (shared folders), другие подразделения и т.д. Создание в домене структуры подразделений позволяет выполнять следующие действия. Эффективно делегировать административные полномочия. Например, можно позволить администратору отдела управлять объектами в собственном подразделении – создавать пользователей и группы, сбрасывать пароли, не предоставляя при этом полных административных прав во всем домене. Централизованно управлять рабочей средой пользователей и настройками компьютеров с помощью групповой политики, привязанной (linked) к определенному подразделению. Разместив учетные записи пользователей и компьютеров в подразделении и привязав к нему групповую политику, можно, например, централизованно установить на компьютеры приложение или скрыть значок «Сетевое окружение» с Рабочего стола. Служба каталога может обеспечить однократную регистрацию в системе (single sign-on). Смысл однократной регистрации состоит в том, что пользователь, один раз регистрируясь в службе каталога, получает доступ ко всем ресурсам сети (например, общим папкам), для которых у него есть соответствующие разрешения. Служба каталогов Active Directory в Windows Server 2003 поддерживает создание доверительных отношений между отдельными доменами разных лесов, а также создание доверительных отношений между самими лесами. Это позволяет пользователям из одного домена получить доступ к ресурсам (общим папкам и принтерам) другого домена.

Безопасность в Active Directory и делегирование административных полномочий

В Active Directory можно выделить две административные группы – Domain Admins и Enterprise Admins. Члены группы Domain Admins (группа существует в каждом

домене) обладают полными административными правами только в своем домене, т.е. могут управлять контроллерами, серверами и клиентскими станциями своего домена. Члены группы Enterprise Admins (группа существует только в корневом домене леса) обладают полными административными правами на всех контроллерах леса, но не могут администрировать серверы и клиентские станции. Согласно рекомендациям компании Microsoft, членство в этих группах должно быть крайне ограничено. Обычные пользователи имеют возможность только читать информацию из Active Directory (с некоторыми ограничениями). Active Directory позволяет выполнить делегирование административных задач пользователям, не предоставляя им членства в группах Domain Admins и Enterprise Admins. Для этой цели применяется Мастер делегирования административных задач (Delegation of Control Wizard). С помощью этого мастера можно делегировать на уровне подразделения как типичные (например, Create, delete, and manage user accounts), так и нестандартные задачи (например, разрешить пользователям изменять свою персональную информацию, такую, как адрес).

Групповая политика в домене Active Directory

Групповая политика (Group Policy) – мощнейший механизм централизованного администрирования в домене Active Directory . С помощью групповой политики можно управлять рабочей средой пользователей (настройки Рабочего стола, меню Пуск, Панели управления и т.д.); безопасностью компьютера (настройки безопасности, выключение ненужных служб, разрешения NTFS и т.д.); установкой и удалением приложений; перенаправлением пользовательских папок на сервер; настройкой программ, таких как Internet Explorer, Microsoft Office и других.

Хранение и порядок применения Групповой политики

Групповая политика – набор настроек, который хранится на контроллерах домена и автоматически загружается и применяется соответствующими компьютерами – членами домена. Термином объект групповой политики (Group Policy object, GPO) обозначается конкретный экземпляр групповой политики, привязанный к домену или подразделению. Объект групповой политики частично хранится в базе Active Directory, но основная его часть хранится в общей папке, доступной для загрузки клиентами (\\\SY$VOL\\Policies\Policy_GUID>).

Структурно групповая политика состоит из двух частей: настройки компьютера (computer configuration) и настройки пользователя (user configuration). Настройки раздела computer configuration применяются к учетным записям компьютеров (computer accounts), а настройки раздела user configuration – к учетным записям пользователей (user accounts). Несмотря на название, настройки групповой политики не применяются к объектам типа группа (groups).

Объект групповой политики может быть привязан в Active Directory на уровне сайта, домена или подразделения. При этом важно понимать, что GPO – это совершенно независимый объект, поэтому один и тот же объект групповой политики может быть привязан сразу к нескольким подразделениям.

По умолчанию порядок применения объектов групповой политики следующий:

1) применяются настройки объекта групповой политики, привязанного к сайту;
2) применяются настройки объекта групповой политики, привязанного к домену;
3) применяются настройки объекта групповой политики, привязанного к вышестоящему подразделению;
4) применяются настройки объекта групповой политики, привязанного к нижестоящему подразделению.

Таким образом, настройки применяются сверху вниз. При этом неконфликтующие настройки суммируются, а для конфликтующих настроек

«побеждают» применившиеся позже (т.е. находящиеся «ближе» к тому объекту, для которого они применяются).

Инструменты для работы с групповой политикой

Microsoft представляет два инструментальных средства для работы с групповой политикой: оснастку Group Policy Editor (входит в состав операционной системы) и административное средство Group Policy Management Console (GPMC). GPMC не входит в состав системы, его можно загрузить с сайта компании Microsoft. GPMC предоставляет большие возможности по управлению групповой политикой, такие как единый просмотр всех объектов групповой политики, удобный интерфейс для привязки и делегирования разрешений на GPO, а также возможность резервного копирования и восстановления GPO. Использование GPMC для управления групповой политикой не обязательно, но крайне рекомендуется.

Изменение порядка применения Групповой политики

Изменить порядок применения Групповой политики можно с помощью блокирования наследования политики (опция Block Policy Inheritance) и с помощью запрета переопределения (опция No Override). Блокирование наследования (Block Policy Inheritance) – опция, устанавливаемая в свойствах подразделения (OU). Если эта опция установлена, то к пользователям и компьютерам этого подразделения применяются только GPO, привязанные непосредственно к этому подразделению. Применение вышестоящих GPO (например, доменных) будет заблокировано. Запрет переопределения (No Override) – опция, устанавливаемая на уровне связи GPO и подразделения, сайта или домена. Установленная опция No Override приводит к тому, что настройки данного GPO не «затираются» настройками нижестоящих GPO, которые применяются позже. Эта опция имеет больший приоритет, чем опция блокирования наследования. Чаще всего опцию No Override устанавливают в сценарии, когда нужно создать GPO, привязанный к домену и содержащий критические настройки, которые должны быть применены ко всем объектам домена независимо от настроек нижестоящих политик и возможного блокирования наследования /2/.

Восстановление данных в Active Directory

В случае какого-либо сбоя в Active Directory информацию можно восстановить с помощью скрипта **mRestore.wsf** из дистрибутива Прометея. В случае версии 4.3 он лежит в папке **bin**, в случае версии 4.2 – в корневом каталоге дистрибутива.

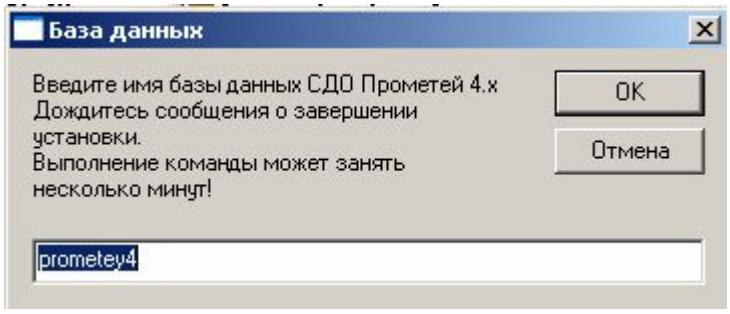

Рис.1. Главное окно скрипта mRestore.wsf

После запуска скрипта в окошке надо указать название инсталляции Прометея, далее ввести цифры в зависимости от требуемого действия. Например, надо восстановить все объекты системы – вводите "1".

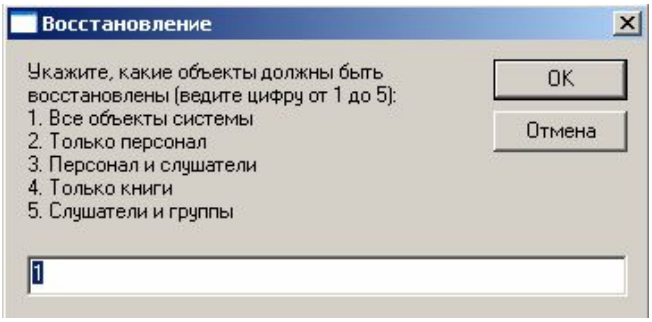

Рис.2. Выбор способа восстановления БД Active Directory

Полученный **total.cmd** надо не запускать, а вставить его текст в командную строку (так как этот файл создается в кодировке Windows), для этого необходимо нажать кнопку Пуск-Выполнить, в строке «Выполнить» прописать cmd и нажать на Enter. После чего нужно нажать сочетание клавиш Ctrl+V или нажать правую кнопку мыши и в вышедшем меню выбрать строчку «Вставить»

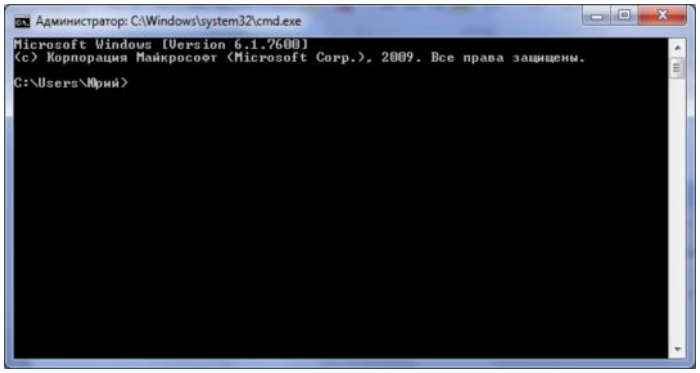

Рис.3. Окно командной строки cmd в Windows Server2003

Список литературы

1. http://www.obrazovanie ufa.ru/Vuz/Dostoinstva_i_nedostatki_distantsionnogo_obucheniya.htm
2. http://www.chla.ru/index.php/about-ad