электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

УДК 004.42

Разработка единой системы управления пользователями в корпоративных приложениях Университета

М.А. Рыбальченко

Студент, кафедра «Программное обеспечение ЭВМ и информационные технологии» МГТУ им. Баумана, г. Москва, Россия

Научный руководитель: Остриков С.П.., к.т.н., доцент кафедры «Программное обеспечение ЭВМ и информационные технологии», г. Москва, Россия

МГТУ им. Н.Э. Баумана
maxim207@mail.ru

Рост количества информационных систем, вовлеченных в процессы работы Университета, делает все более актуальным вопрос контроля и управления доступом к информационным ресурсам (ИР). Также при постоянном увеличении числа отделений, ростом числа сотрудников и их частой миграцией между отделениями, возникает потребность в решениях автоматизации процессов управления учетными записями и идентификационными данными пользователей.

Внедрение решений по управлению пользователями, или *Identity Management(IdM)*-решений, обеспечивает эффективную реализацию многих задач и позволяет в значительной степени оптимизировать управление ИТ-инфраструктурой Университета. Кроме того, в России, как и на Западе, появилось множество законодательных актов, прямо или косвенно указывающих на необходимость внедрения подобных систем, например *Sar-banes-Oxley Act*, серия международных стандартов ISO 2700X, различные требования и рекомендации по построению информационных систем, такие как *CoBIT, ITIL* и пр. Стоит отдельно отметить *федеральный закон РФ №152-ФЗ "О персональных данных"*, существенную часть требований которого можно реализовать путем внедрения *IdM*-решения[1].

Для решения проблемы управления пользователями необходимо реализовать следующие задачи:

- Автоматизация процессов авторизации новых сотрудников к ресурсам Корпоративных Информационных Систем (КИС);
- Обработка и контроль изменений кадровой информации, необходимой для регулирования прав доступа пользователей;
- Создание единой системы управления учетными записями и правами пользователей в КИС;
- Построение централизованного хранилища информации учетных данных и прав пользователей в КИС;
- Повышение уровня информационной безопасности путем четкого разграничения прав пользователей на доступ к информации;
- Сокращение ручного труда за счет автоматизации изменений прав доступа в КИС;

Свои решения в области *Identity Management* представили практически все лидеры рынка, такие как *Sun Microsystems, Oracle, IBM, Novell* и другие[1]. Базовая функциональность этих решений примерно одинакова: среда выполнения процессов, процессы согласования предоставления и изменения доступа, управление паролями и набор «стандартный коннекторов»[1]. Оценочная стоимость использования лицензий таких решений для вуза, в котором количество пользователей исчисляется тысячами, достигает сотен тысяч долларов в год[2].

Перечислим набор функций *Identity Management*, критически важных с точки зрения приемлемости Университета, в частности[3]:

- отсутствие глобальной единой точки отказа для доступа пользователей к приложениям, с одной стороны, и максимальная централизация *IdM* для эффективного управления корпоративными пользователями - с другой;
- гарантированная безопасность самого *IdM*-решения, концентрирующего в одной точке ранее разрозненную конфиденциальную информацию о пользователях и ИТ-ресурсах;
- простота, быстрота и безопасность реального внедрения (с точки зрения влияния на нормальную работу ресурсов);
- масштабирование до десятков тысяч пользователей;
- возможность внедрения и управления действующими ИТ-ландшафтами без необходимости их модификации и подстройки под выбранную *IdM*-платформу, в крайнем случае, с минимально возможной подстройкой (безагентные адаптеры управляемых ресурсов);

- эффективное функционирование в условиях регулярных изменений (патчи, апгрейды) управляемых ресурсов после внедрения *IdM.*

Разработка собственного *Identity Management* решения позволит решить все поставленные задачи с учетом специфики существующей IT-инфраструктуры, а также существенно сократить затраты на внедрение и поддержку системы управления пользователями.

Также разработанная система, помимо решения проблемы управления пользователями, может быть использована как основа для решения ряда других проблем, в частности управления лицензиями на программное обеспечение[5].

Службы каталогов

В настоящее время большинство служб каталогов различных фирм базируются на стандарте *X.500.* Для доступа к информации, хранящейся в службах каталогов, обычно используется протокол *Lightweight Directory Access Protocol* (*LDAP*). В связи со стремительным развитием сетей *TCP/IP*, протокол *LDAP* становится стандартом для служб каталогов и приложений, ориентированных на использование службы каталога.

Служба каталогов *Active Directory(AD)* является основой логической структуры корпоративных сетей, базирующихся на системе *Windows*. Термин "*Каталог*" в самом широком смысле означает "*Справочник*", а служба каталогов корпоративной сети — это централизованный корпоративный справочник. Корпоративный каталог может содержать информацию об объектах различных типов. Служба каталогов *Active Directory* содержит в первую очередь объекты, на которых базируется система безопасности сетей *Windows*, — учетные записи пользователей, групп и компьютеров. Учетные записи организованы в логические структуры: *домен, дерево*, лес, организационные подразделения[4].

Преимущества использования Active Directory[4]:

- **Единая точка аутентификации.** При использовании домена Active Directory все учётные записи пользователей хранятся в одной базе данных, и все компьютеры обращаются к ней за авторизацией.
- **Единая точка управления политиками.** Все пользователи и компьютеры иерархически распределяются по организационным подразделениям, к каждому из которых применяются единые групповые политики. Политики позволяют задать единые настройки и параметры безопасности для группы компьютеров и пользователей.
- **Единая регистрация**. Пользователи могут войти в сеть с помощью идентификации основных пользовательских имен *(UPN -User Principal Name),*

например, *mike@contoso.com*. После успешной идентификации им будет предоставлен доступ ко всем сетевым ресурсам, для которых им было дано разрешение, без необходимости регистрироваться снова на различных серверах или доменах.

- **Интегрированная безопасность.** Служба Active Directory использует подсистему безопасности Windows Server при аутентификации пользователей и обеспечении защиты общедоступных сетевых ресурсов.
- **Масштабируемость.** Поскольку организация постепенно растет в процессе своего развития, служба Active Directory спроектирована масштабируемой, для того чтобы справляться с этим ростом. Вы можете расширить размер доменной модели или просто добавить больше серверов, чтобы приспособиться к потребностям увеличения объема.
- **Поддержка служб сертификации.** Можно использовать службы сертификатов Active Directory для создания одного или нескольких центров сертификации, которые будут получать запросы на сертификаты, проверять данные запросов, идентифицировать запрашивающую сторону, выдавать сертификаты, отзывать сертификаты и публиковать данные об отзывах сертификатов.

Создание структуры Университета в Active Directory

Для хранения информации учетных данных и прав пользователей в КИС был сформирован кадровый справочник МГТУ им. Баумана в *Microsoft Active Directory*. Структура справочника представляет отдельную ветку *(Organizational Unit, OU)* в корне с именем «BMSTU». Кадровый справочник содержит следующие разделы:

- Иерархический классификатор структуры подразделений МГТУ им. Н.Э. Баумана *OU «ORG».*
- Иерархический классификатор профессий МГТУ им. Н.Э. Баумана OU «PROF»
- Список сотрудников *OU «USR».*

Для объектов справочника, которые ранее существовали, но в настоящее время отсутствуют в кадровой системе (уволенные сотрудники, расформированные структурные подразделения и т.д.) в корне *Active Directory* сформирован аналогичный справочник для удаленных объектов *OU «BMSTU-DEL»* с аналогичной иерархической структурой *OU «ORG-DEL», OU «PROF-DEL», OU «USR-DEL»*. Структура иерархических классификаторов спроектирована таким образом, что позволяет создавать связи типа «один к одному», «один ко многим», «многие ко многим» с объектами других классификаторов кадрового справочника МГТУ им. Н.Э. Баумана в *Active Directory*.

Задача отнесения сотрудников к одной и более должностям/структурным подразделениям решается через членство учетных записей сотрудников в универсальных группах безопасности *AD DC* относящимся к данным должностям/структурным подразделениям:

- В структуре *Active Directory* создается корневая ветка *BMSTU*, внутри которой создаются три вложенных ветки:
  - *«ORG»;*
  - *«PROF»;*
  - *«USER».*
- В ветке *«ORG»* формируется иерархическая структура подразделений *(OU).* В каждом подразделении создается группа (универсальная группа безопасности) с одноименным названием.
- В ветке *«PROF»* формируется список должностей *(OU)*, внутри каждой должности создается группа (универсальная группа безопасности) с одноименным названием.
- В ветке *«USER»* создаются пользователи. В зависимости от принадлежности пользователя к тому или иному подразделению, он включается в соответствующую группу подразделения. Сотрудник включается в группы безопасности, соответствующие должностям, которые он занимает в настоящее время.
- В корне *Active Directory* создается еще одна ветка, имеющая название *«del_BMSTU»,* с тремя вложенными ветками:
  - *«ORG»;*
  - *«PROF»;*
  - *«USER».*
- При удалении *OU* подразделения оно перемещается на ветку *del_BMSTU\ORG*. При удалении *OU* должности она перемещается на ветку *del_BMSTU\PROF*. При удалении *CN* сотрудника, у соответствующей ему учетной записи устанавливается состояние «Не активен/отключен» (*userAccountControl = 546*), и учетная запись перемещается на ветку *del_BMSTU\USR*.
- При исключении сотрудника из подразделения, или смены должности, учетная запись удаляется из соответствующих групп безопасности *Active Directory*.

Рисунок 1 отображает структуру *OU* ветки *«BMSTU»,* относящиеся к ним группы безопасности и пользователей. Также на данном рисунке отображено отношение пользователей к группам безопасности (должностей и структурных подразделений).

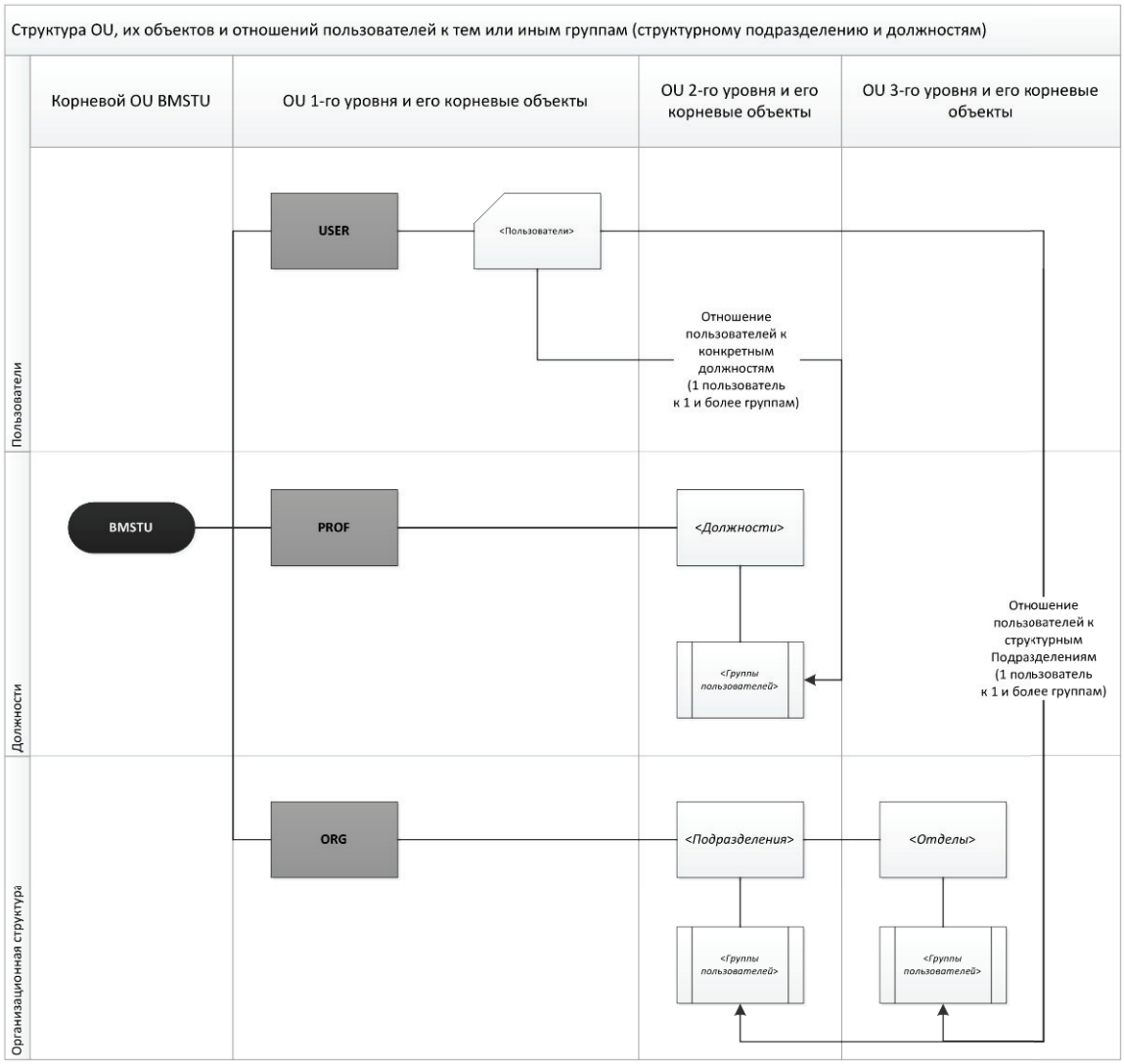

Рис. 1. Структура OU, их объектов и отношений пользователей к тем или иным группам (структурному подразделению и должностям)

Полученная структура подразделений Университета в Active Directory показана на рисунке 2. Здесь отображено, как отделы и подразделения (*OU*) формируют иерархический классификатор. Также в каждом подразделении присутствует одноименная группа безопасности (*Security Group*).

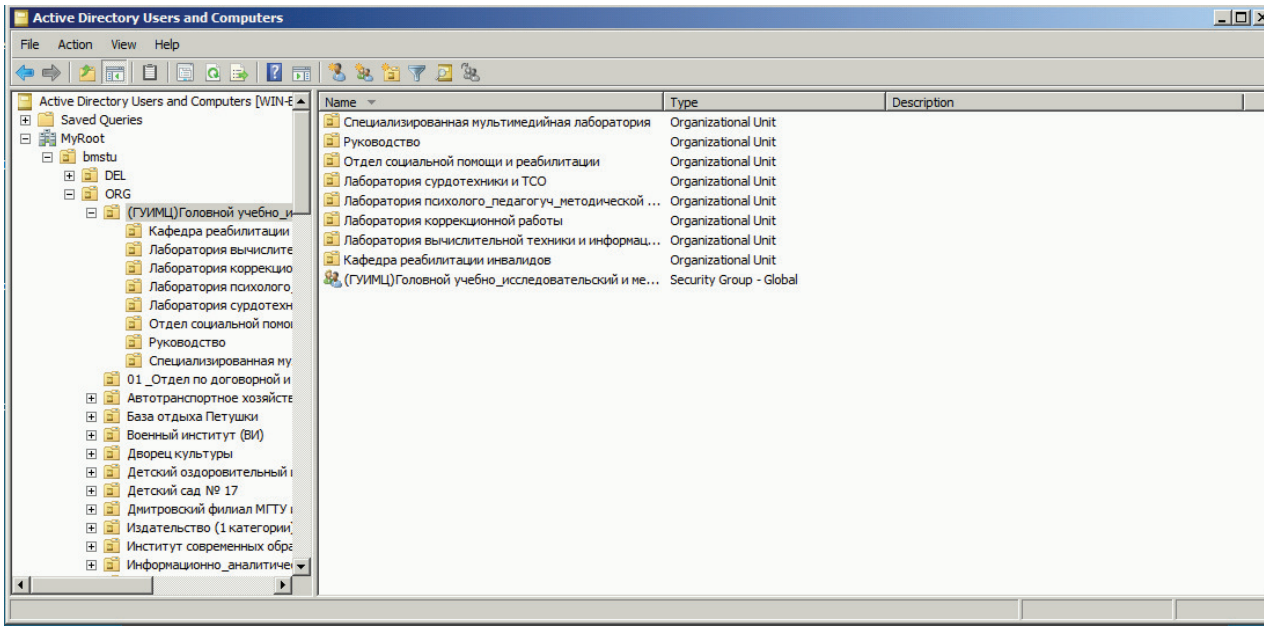

Рис. 2. Структура ORG, иерархическая структура подразделений в службе каталогов Active Directory

На рисунке 3 отображен классификатор профессий Университета. OU каждой должности, помимо одноименной группы безопасности, имеет перечень всех вакансий, соответствующей данной должности. Каждая вакансия состоит в группе подразделения из ORG, к которому эта вакансия относится.

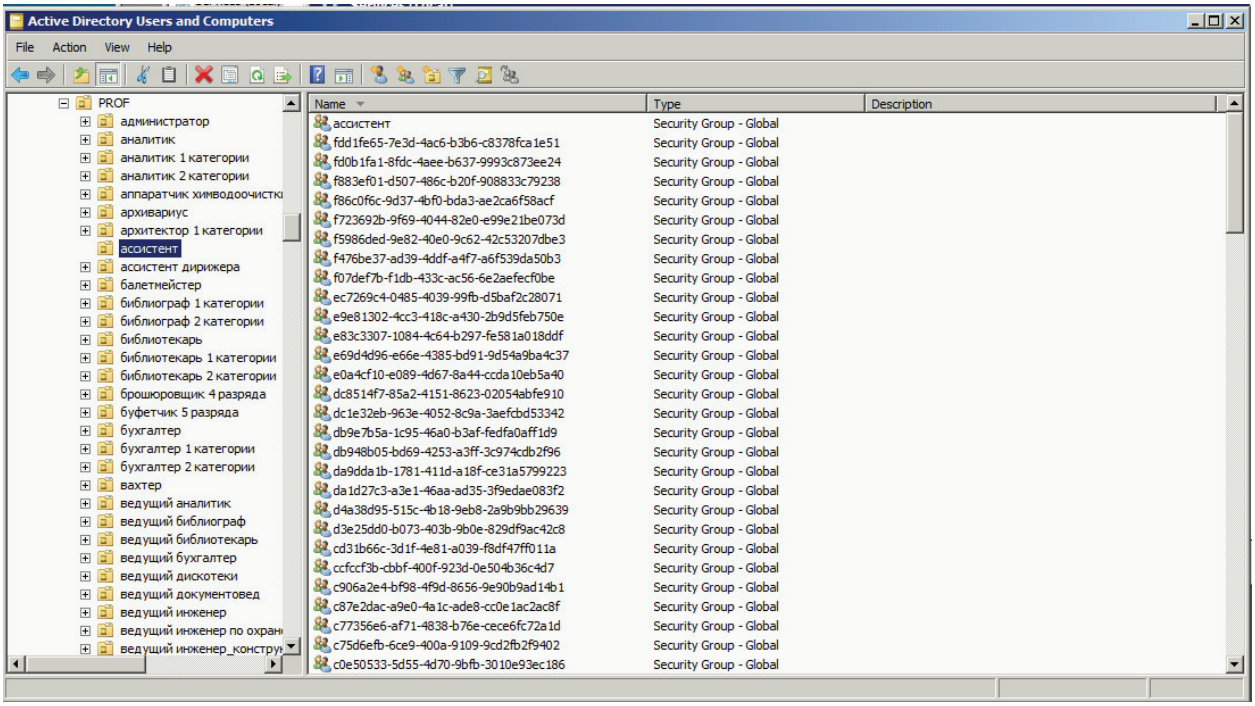

Рис. 3. Структура PROF, перечень должностей и вакансий Университета в службе каталогов Active Directory

Интеграционный сервис

Для синхронизации данных между кадровой системой и справочником в *AD* был разработан интеграционный сервис, который представляет собой системную службу *Windows*. Службе ИС могут быть посланы команды запуска, остановки, приостановки и возобновления выполнения; также возможно выполнение команд к немедленному запуску сеанса синхронизации. ИС поддерживает, как автоматический запуск сеанса синхронизации по настроенному расписанию, так и запуск сеанса синхронизации по требованию – вручную.

Автоматический запуск осуществляется службой *Windows*, которая по заранее настроенному расписанию запускает сеанс синхронизации.

В случае необходимости ручного запуска администратор может ввести команду, которая будет воспринята интеграционным сервисом (системной службой) как команда к немедленному запуску сеанса синхронизации (используется компонент *ServiceController*).

Для получения актуальных данных о пользователях интеграционный сервис подключается к файловому серверу и осуществляет поиск и импорт файлов *persons.xml* и *struct.xml* имеющих дату создания наиболее близкую к текущей дате. ИС загружает данные из файлового сервера по протоколу *FTP*. Путь к файлам *persons.xml* и *struct.xml*, размещенным на файловом сервере, имеет следующий вид:

ftp://<Имя_Сервера>/XML/UEF/KDR/<дата(ГГГГ-ММ-ДД)>_<время(ЧЧ-ММ-СС)>/<дата(ГГГГ-ММ-ДД)>.

Из содержимого полученных по FTP файлов *persons.xml* и *struct.xml* извлекается вторая строка дата создания *(<struct date="2012-12-15">)*. Интеграционный сервис производит сравнение извлеченной из содержимого файла даты с датой последнего успешного сеанса синхронизации. Извлеченные из файлов stuct.xml и persons.xml даты должны совпадать. В случае если даты не совпадают, то сеанс синхронизации завершается. Информация о досрочном завершении сеанса синхронизации записывается в журнал событий ИС (*Сеанс синхронизации досрочно завершен! Даты файлов не совпадают, дата struct.xml "2012-12-10", дата persons.xml "2012-12-11").*

В случае если вновь полученные файлы stuct.xml и persons.xml были созданы раньше, чем дата последнего успешного сеанса синхронизации, то сеанс синхронизации завершается. Информация о досрочном завершении сеанса синхронизации записывается в журнал событий ИС (Сеанс синхронизации досрочно завершен! Дата последней успешной синхронизации "2012-12-15", дата *struct.xml* "2012-12-10", дата *persons.xml*

"2012-12-10".

При запуске синхронизации интеграционный сервис производит анализ данных, содержащихся в файлах *struct.xml* и *persons.xml*, сопоставляет данные о структуре, должностям (профессиям), сотрудникам с данными содержащимися в *«ou BMSTU» Active Directory*. Для обработки содержимого *XML*-файлов используются библиотеки пространства имен *System.Xml Microsoft .NET Framework 4.0.*

Структура файлов struct.xml и persons.xml

Файл *persons.xml*, содержащий следующие данные о сотрудниках:

- фамилия (lastname);
- имя (firstname);
- отчество (middlename);
- пол (gender);
- дата рождения в формате «год-месяц-число» (birthday);
- идентификационный номер подразделения (guid);
- должность (prof);
- идентификатор профессии 1 уровня (profguid);
- идентификатор профессии 2 (vacguid);
- идентификатор конкретного подразделения в ИТ системах организации (struct guid);
- идентификатор пользователя в ПО автоматизации кадрового учета (id);
- идентификатор глобального учета пользователей в ИТ системах организации(guid);
- тип ставки оплаты труда (marks).

Данные об иерархической организационной структуре МГТУ им Н.Э. Баумана экспортируются из системы «АБ-кадры» в виде файла *struct.xml*, содержащего следующие сведения об организационной структуре:

- уникальный идентификатор подразделения в кадровой системе организации (id);
- вспомогательный идентификатор подразделения в кадровой системе организации (number);
- наименование подразделения (name);
- идентификатор конкретного подразделения в ИТ системах организации (struct guid);

- идентификационный номер подразделения (guid);
- наименования вакансий (штатных должностей согласно официальному штатному расписанию организации в данном структурном подразделении (vacancy guid);
- идентификатор профессии (professionUID), связан с идентификатором профессии 1 уровня (profguid) (professionUID = profguid).

Обновление данных кадрового справочника

По результатам анализа ИС формирует список объектов и атрибутов данных подлежащих обновлению в кадровом справочнике МГТУ им. Н.Э. Баумана в Microsoft *Active Directory* (Далее - Список обновления).

В случае если по результатам анализа сформировался нулевой Список обновления (нет объектов подлежащих обновлению), то сеанс синхронизации завершается. Информация о досрочном завершении сеанса синхронизации записывается в журнал событий ИС (Сеанс синхронизации досрочно завершен! Список обновления не содержит объектов подлежащих обновлению).

Если по результатам выполнения предыдущей процедуры, сформировался не нулевой Список обновления, то выполняется процедура обновления данных. В зависимости от содержания Списка обновления, интеграционный сервис должен произвести создание нового объекта, изменение или перемещение существующего объекта в другой *OU*.

При выполнении сеанса синхронизации, в первую очередь осуществляется синхронизация организационной структуры (ветка *ORG*), затем профессий (ветка *PROF*), затем учетных записей пользователей (ветка *USER*).

Если на момент начала сеанса синхронизации объект не содержится в кадровом справочнике МГТУ им. Н.Э. Баумана в *Microsoft Active Directory*, то ИС создает его, используя метод *DirectoryEntry.Children.Add*. После создания нового объекта ИС обеспечивает установление требуемых связей данного объекта с другими объектами в кадровом справочнике МГТУ им. Н.Э. Баумана через членство данного объекта в необходимых группах безопасности других веток.

Контроль за успешность создания нового объекта осуществляется на основании параметров *highestCommittedUSN, uSNCreated, whenCreated*.

Если Список обновления содержит объект, который уже присутствует в кадровом справочнике МГТУ им. Н.Э. Баумана в службе каталогов *Microsoft Active Directory*, но

отличается отдельными параметрами (атрибутами). В этом случае, ИС не создает новый объект, а выполняет изменение требуемых параметров в существующем объекте в кадровом справочнике МГТУ им. Н.Э. Баумана в службе каталогов *Microsoft Active Directory*. Для этого ИС использует метод *DirectoryEntry.Properties["<имя свойства>"].Value = <значение свойства>*.

По окончанию выполнения функций обновления, результаты работы сервиса записываются в журнал событий (Рис. 4).

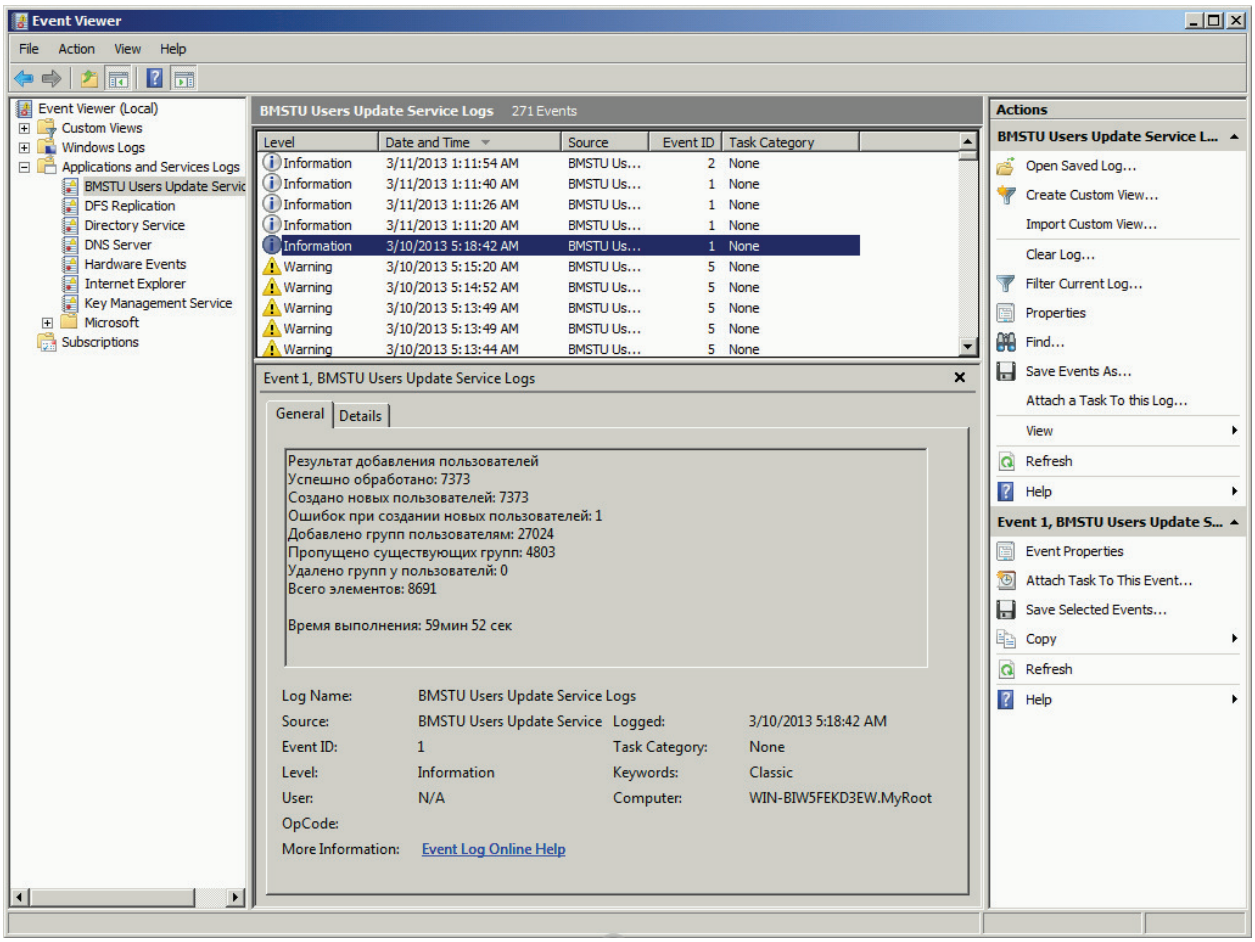

Рис. 4. Отчет о результатах выполнения операции добавления пользователей в журнале событий Event Viewer

Измерение производительности

Для исследования работы интеграционного сервиса был использован инструмент *Performance Monitor*. Эта утилита поставляется вместе с ОС Windows Server, и позволяет предоставлять результаты измеряемых метрик в виде графиков или отчета. Преимуществом этого инструмента является то, что он надежно интегрируется с операционными системами Windows и поэтому отображает достоверные значения

различных аспектов производительности. Performance Monitor предоставляет множество объектов производительности, и каждый объект производительности имеет несколько счетчиков. [6]

Были использованы следующие счетчики:

- **ADs \LDAP Search/sec** – число операций поиска в секунду, выполняемых для запросов по протоколу *LDAP*. Является хорошим индикатором интенсивности использования контроллера домена. При оптимальной структуре службы каталогов метрика должна иметь одинаковое значение для всех контроллеров домена. Увеличение значения метрики указывает на то, что в сети появилось новое приложение, работающее со службой каталогов, или возросло количество клиентских компьютеров.
- **DS Directory Writes/Sec** – число операций записи в каталог *AD* в секунду
- **DS Directory Reads/Sec** – число операций чтения из каталога *AD* в секунду

Сначала было произведено измерение активности системы в то время, когда сервис не выполняет функции работы с AD. Такой уровень активности обозначим как базовый для данной системы. Базовый уровень представляет собой уровень индикатора функционирования, соответствующий пределам нормальной работы системы. Пределы нормальной работы должны включать и низкие, и высокие значения, которые ожидаются для определенного счетчика. Чтобы точнее фиксировать базовые данные, необходимо собирать информацию о работе системы в течение достаточно длительного периода времени, чтобы отразить диапазон значений. Например, если требуется установить базовый уровень производительности для аутентификационных запросов, необходимо отслеживать значения этого индикатора в те периоды времени, когда большинство пользователей входит в систему.

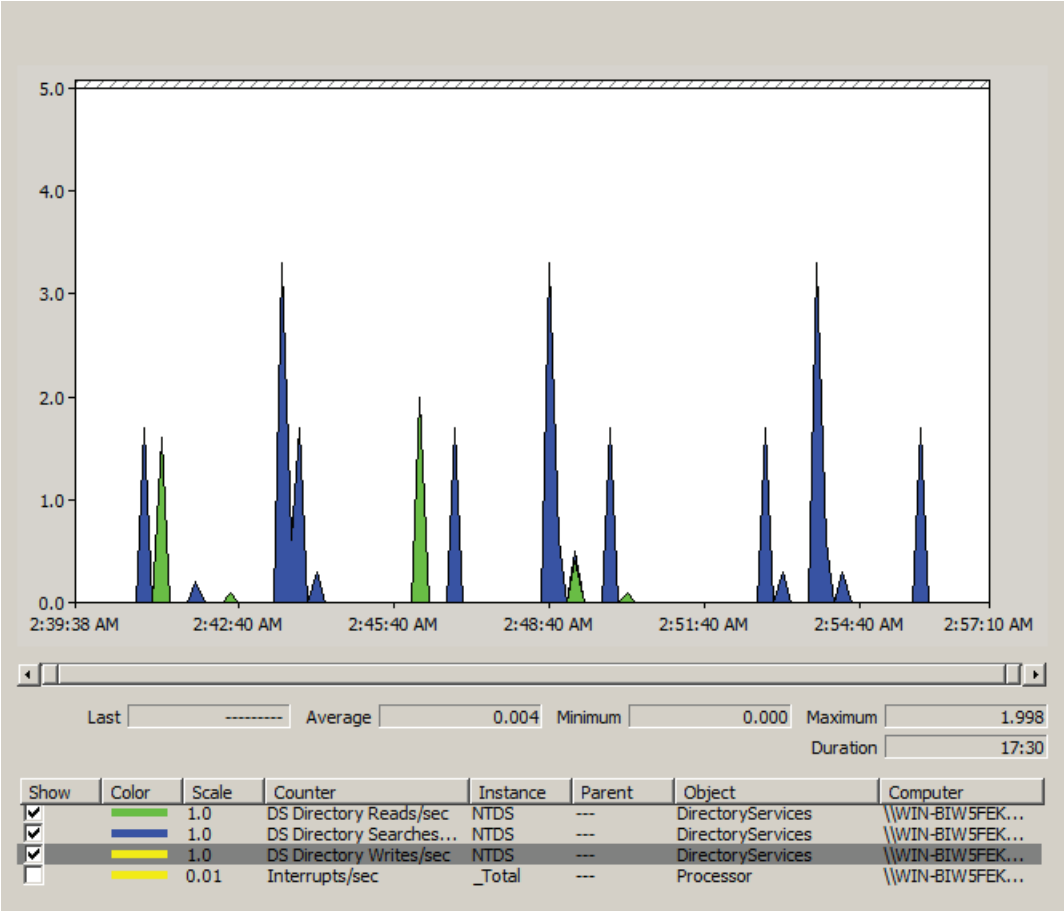

Рис. 5. Измерение активности Active Directory во время остановки работы интеграционного сервиса

На рисунке 5 видно, что активность обращений к *Active Directory* в базовом режиме невысокая. Измерения производились на виртуальной машине под управлением Windows Server 2008 R2. Видна некоторая периодичность выполнения операций, связанная с работой служб Active Directory. В остальное время количество обращений к службе каталогов нулевое.

После установки интеграционного сервиса в системе, и запуске функций обновления получаем следующие результаты:

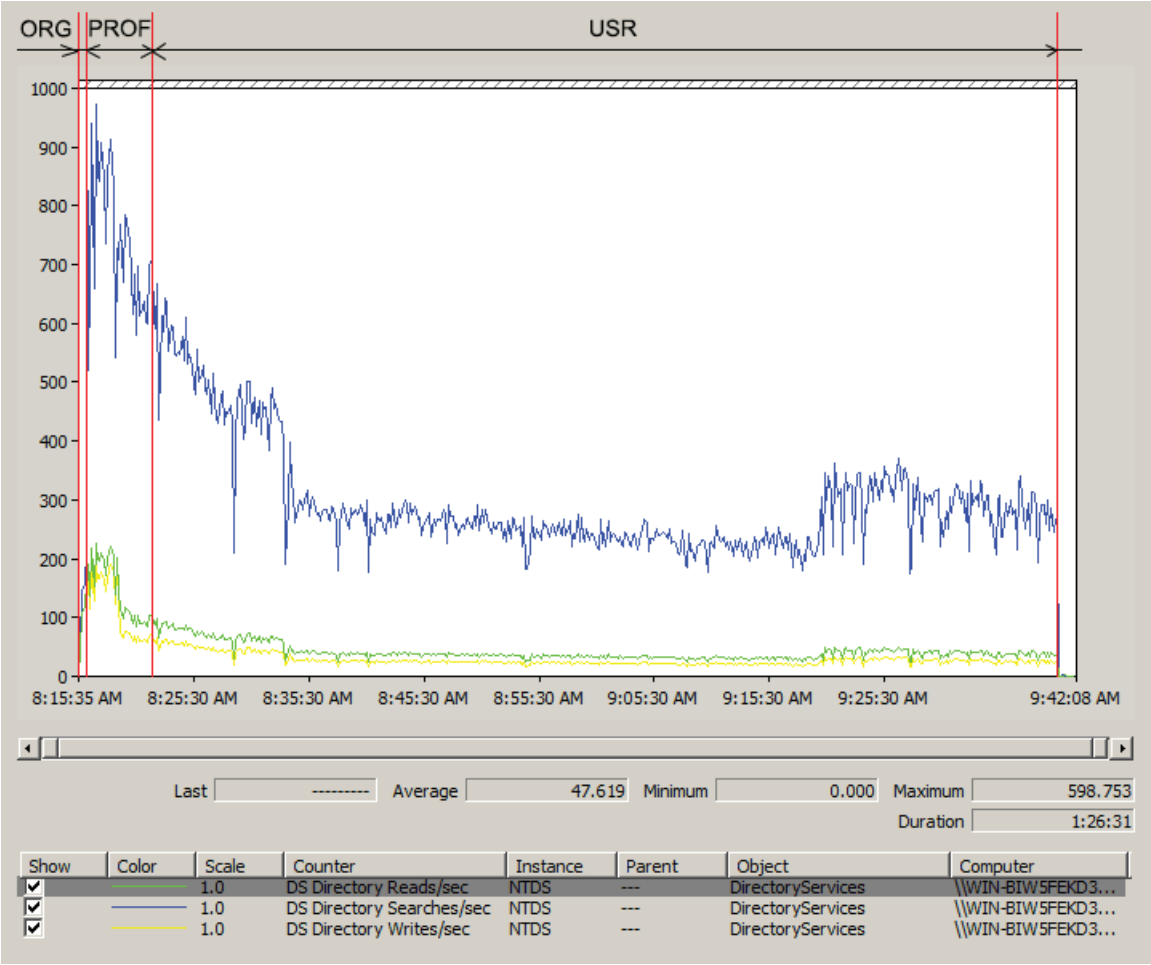

Рис. 6. Измерение активности Active Directory во время выполнения обновления интеграционным сервисом структур ORG, PROF, USR.

Рисунок 6 отображает весь период создания структур ORG, PROF и USR. Полученные метрики отражены в таблице 1.

Таблица 1

Показания счетчиков при выполнении обновления интеграционным сервисом

Структура	**DS Directory Searchs/Sec**			**DS Directory Writes/Sec**			**DS Directory Reads/Sec**			**Время выполнения (ч:мин:сек)**
	MIN	*MAX*	*AVE*	*MIN*	*MAX*	*AVE*	*MIN*	*MAX*	*AVE*	
ORG	43	340	163	42	340	163	32	261	122	00:00:34
PROF	134	1526	741	0	235	114	0	263	145	00:02:44
USR	0	1542	294	0	333	27	0	598	40	01:20:22
ВСЕГО:	0	1542	317	0	342	33	0	598	48	01:23:40

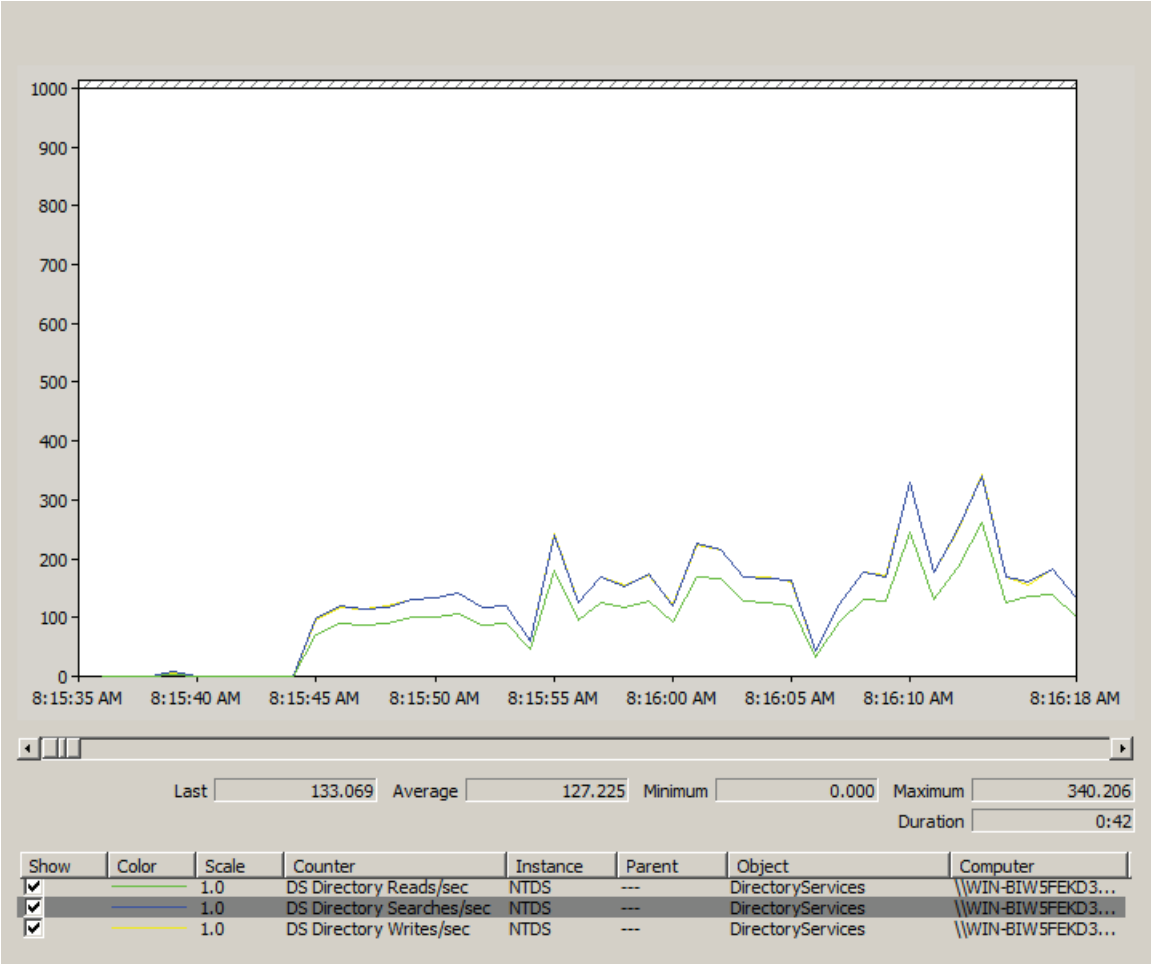

Рис. 7. Измерение активности Active Directory во время выполнения обновления интеграционным сервисом каталога ORG

На этапе развертывания ORG происходит создание структуры подразделений Университета. Количество операций поиска (Searchs) в AD на данном этапе совпадает с числом операций записи (Writes)(см. рисунок 7). Это связано с тем, что при создании нового OU структуры ORG выполняется поиск в AD, чтобы предотвратить повторное создание одноименных OU.

Рис. 8. Измерение активности Active Directory во время выполнения обновления интеграционным сервисом каталога PROF

При создании структуры PROF отмечается высокое число операций поиска при обращении к AD. На данном этапе выполняется создание классификатора профессий, вакансий и установление связей с структурой ORG. Поэтому количество операций поиска и записи высоко. Также число операций чтения выше, чем операций записи, так как помимо создания PROF происходит чтение данных из ORG.(рисунок 8)

Рис. 9. Измерение активности Active Directory во время выполнения создания интеграционным сервисом пользователей в каталоге USR

Во время этапа добавления пользователей наблюдается скачек активности в начале выполнения, так как перед началом обновления формируется список существующих пользователей. Использования этого списка избавляет сервис от постоянного выполнения проверки на существование текущего обрабатываемого пользователя, тем самым уменьшая число *Searchs* на протяжении всего выполнения этапа добавления пользователей.

В конце выполнения происходит перемещение уволенных пользователей в *OU DEL*, их деактивация и очищение их списка групп. Повышенная активность работы с *AD*, связанная с этим процессом наблюдается на рисунке 9.

Этап добавления пользователей занимает значительную часть времени процедуры обновления интеграционного сервиса. Добавление пользователей происходит последовательно, и чтобы сократить время выполнения следует распараллелить этот процесс.

Для распараллеливания выполнения функции добавления пользователей

использовался метод *Parallel.ForEach* пространства имен *System.Threading.Tasks*. Результат выполнения этапа обновления с использованием распараллеливания представлен на рисунке 10.

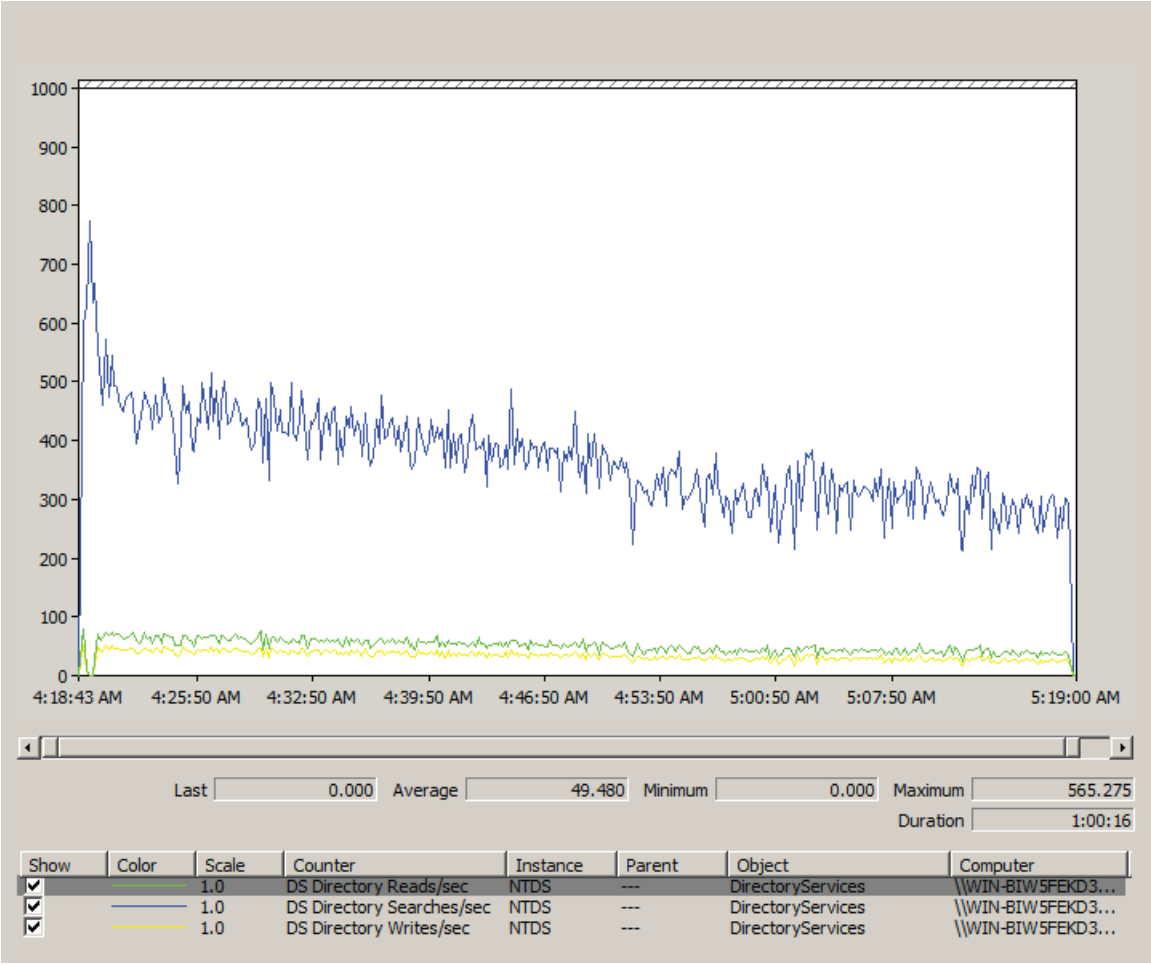

Рис. 10. Измерение активности Active Directory во время выполнения обновления интеграционным сервисом каталога USR с использование распараллеливания

Из таблицы 2 видно, что время выполнения операции выполнения сократилось за счет использования распараллеливания. При этом нагрузка на *AD* распределилась равномерно на протяжении всего обновления (рисунок 10), так как механизм работы *Parallel.ForEach* при создании новых потоков старается распределить нагрузки и ресурсы между ними.

Таблица 2

Показания счетчиков при выполнении обновления USR интеграционным сервисом с использование распараллеливания

Структура	**DS Directory Searchs/Sec**			**DS Directory Writes/Sec**			**DS Directory Reads/Sec**			**Время выполнения (ч:мин:сек)**
	MIN	*MAX*	*AVE*	*MIN*	*MAX*	*AVE*	*MIN*	*MAX*	*AVE*	
USR	0	1622	364	0	550	33	0	565	49	01:00:16

Выводы

С ростом числа сотрудников и корпоративных приложений в Университете возникает проблема управления пользователями и наделении их правами. Внедрение готовых *IdM*-решений позволяет решать поставленные задачи, однако организация управления большими системами остается одной из немногих областей, где невозможно предложить полностью готовые решения; здесь всегда необходим творческий подход и учет всех уникальных особенностей конкретной системы.

Внедрение собственной системы на основе службы каталогов *Active Directory* позволит организовать работу по управлению учетными записями пользователей по принципу *AAA (Authentication, Authorization, Accounting).* Преимущества такого решения:

- Разработанная система учитывает специфику существующей IT-инфраструктуры, отсюда следует простота и быстрота реального внедрения в существующие процессы;
- Наделение правами доступа сотрудников по ролевой модели, согласно должности и структурной принадлежности;
- Обеспечение единого контроль информационной безопасности с точки зрения доступа во все информационные системы (аутентификация и авторизация);
- Контроль изменения кадровой информации избавляет администратора от «ручного» регистрирования пользователей в системе;
- Централизованный автоматический контроль за правами доступа сотрудников к КИС, оказывает положительное виляние на информационную безопасность. К примеру, при увольнении сотрудника система производит автоматическую деактивацию учетных записей пользователей, тем самым, устраняя возможность несанкционированного доступа в КИС, а автоматическая авторизация исключает возможность попадания идентификационных данных пользователя лицам, не

имеющим соответствующих прав доступа;

- Стоимость внедрения и поддержки ниже стоимости лицензий существующих готовых решений.
-

Список литературы

1. «Рынок Решений Identity Management», Jet Info №5, май 2010 г., «Инфосистемы Джет» URL: http://www.jetinfo.ru/jetinfo_arhiv/identity-management-tsentralizovannoe-upravlenie-dostupom/rynok-reshenij-identity-management/2010, (дата обращения 01.03.2013).
2. Материалы Oracle Identity Management, URL: http://oracle.axoft.ru/catalog/product.php?ID=500, (дата обращения 01.03.2013).
3. А.Лаврухин, В.Буряков, «Опыт практического внедрения Identity Mangement-решений в крупных организациях», Журнал "Information Security/ Информационная безопасность" #2, 2008.
4. Статья «Зачем в компании Active Directory?» , URL: http://www.microsoft.com/ru-ru/business/smb/blog/post-view.aspx?id=03, (дата обращения 01.03.2013).
5. М.Козлов, «Разработка системы управления лицензиями на программное обеспечение в техническом Университете», МГТУ им. Баумана, 2013.
6. Статья «Обзор Perfomance Monitor», URL: http://serversql.ru/nastrojka-proizvoditelnosti/obzor-performance-monitor.html, (дата обращения 09.03.2013).