УПРАВЛЕНИЕ ДАННЫМИ УЧЕТНЫХ ЗАПИСЕЙ ПОЛЬЗОВАТЕЛЕЙ ДОМЕНА С ПОМОЩЬЮ FOREFRONT IDENTITY MANAGER

Ю. В. Зверьков, А. В. Кузнецов, М. М. Захаров, М. Ю. Осипов, И. Л. Бондарь

ФГУП «РФЯЦ-ВНИИЭФ», г. Саров Нижегородской обл

Введение

Управление доступом и полномочиями на предприятии должно быть эффективным, рентабельным и безопасным. Между тем, сложность такого управления и обеспечения безопасности пользователей, устройств и служб все возрастает. Это может происходить просто по мере роста предприятия, но может быть и следствием появления новых нормативных документов. В результате, предприятие часто не получает той выгоды, которую должно было бы получить.

Microsoft Forefront Identity Management 2010 R2 (далее FIM 2010 R2) – программный продукт для решения задач управления учетными записями и идентификационной информацией пользователей.

FIM 2010 R2 сильно упрощает процессы управления идентификацией и доступом пользователей благодаря предоставлению портала самообслуживания для пользователей и целому набору инструментов для администраторов, позволяющих автоматизировать типовые задачи по управлению учетными записями, паролями, группами и списками рассылки, а также цифровыми сертификатами пользователей.

В целом, основными задачами FIM являются:

– увеличение эффективности системы управления учетными записями и доступом, снижение текущих расходов предприятий на решение этих задач;

– усиление безопасности;

– снижение нагрузки на ИТ-департамент;

– увеличение производительности труда сотрудников.

Архитектура Forefront Identity Management

FIM 2010 R2 поставляется с готовым набором модулей взаимодействия (Агентов управления) с различными системами, в которых может храниться и обрабатываться идентификационная информация. Архитектура FIM 2010 R2 представлена на рис. 1.

Вместе FIM Service и служба синхронизации (FIM Sync) образуют платформу управления идентификацией (IDM). FIM Service предоставляет механизм обработки запросов через рабочие процессы, и в значительной степени контролирует все, что происходит в службе синхронизации. Служба синхронизации взаимодействует с различными системами

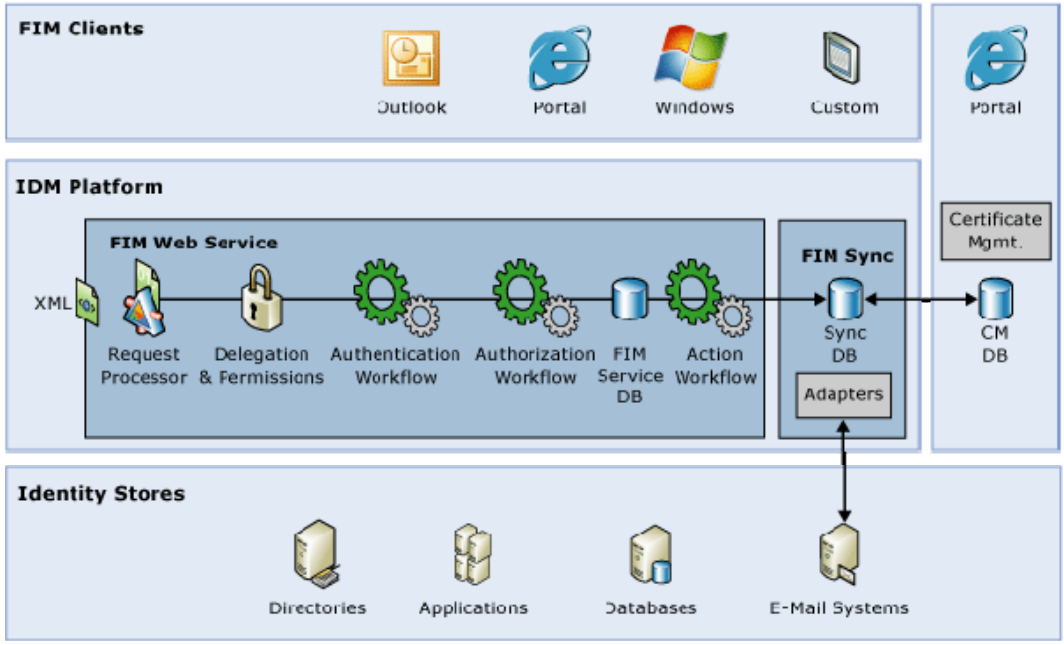

Рис. 1. Архитектура Forefront Identity Management 2010 R2

и источниками данных через адаптеры, называемые агенты управления. Агенты управления являются программными модулями, которые осуществляют подключение и обмен данными между службой синхронизации FIM и целевыми системами, такими как Active Directory, базы данных HR, LDAP и другими.

Компоненты Forefront Identity Management

Forefront Identity Management 2010 R2 состоит из трех основных компонентов:

- FIM Synchronization Service;
- FIM Service;
- FIM Portal.

FIM Synchronization Service

FIM Synchronization Service – централизованная служба, которая хранит и интегрирует информацию из нескольких источников идентификационной информации предприятия. FIM Synchronization Service обеспечивает единое представление всех подключенных источников идентификационных данных, которые могут быть связаны с пользователями, приложениями и сетевыми ресурсами.

Основные объекты FIM Synchronization Service:

- агент управления (Management Agent – MA);
- подключенный каталог (Connected Directory – CD);
- пространство имен агента управления (Connector Namespace – CS);
- пространство имен метастрок (Metaverse Namespace – MV);
- метакаталог (Metadirectory);
- атрибуты (Attributes).

Получая идентификационные данные от подключенных источников информации с помощью управляемых агентов (коннекторов), служба управляет информацией и хранит ее в пространстве коннектора как объекты его буферной зоны. Затем объекты буферной зоны коннектора сопоставляются с записями в метакаталоге (метавселенной), т. е. объектами метакаталога.

Для синхронизации данных между разнородными источниками информации внутри сервиса синхронизации необходима инфраструктура, состоящая из объектов пространства агентов управления, метакаталога и связей между ними. На рис. 2 представлено взаимодействие компонентов в процессе синхронизации одного источника данных с другими.

FIM использует СУБД Microsoft SQL Server для хранения данных. База данных может быть проиндексирована для ускоренного поиска, сервер располагает набором инструментов для мониторинга, сопровождения и восстановления данных.

FIM Service

FIM Service – веб-сервис, предоставляющий централизованные функции управления доступом к информационным ресурсам предприятия на основе запросов. Этот веб-сервис реализует модель обработки запроса, которая содержит три различных этапа рабочего процесса: аутентификацию, авторизацию и действие. Рабочие процессы (каждый из которых содержит один или более видов операций) могут быть прикреплены к каждому из этих шагов и запущены в контексте выполнения одного запроса на доступ к защищенным идентификационным ресурсам.

FIM Portal

FIM портал – веб-сайт, предоставляющий администратору возможности выполнения операций над учетными данными пользователей, группами, возможности управления политиками, а также для решения общих административных задач.

Рис. 2. Пример синхронизации баз данных в FIM 2010

FIM Password Reset Portal также содержит общий для пользователей интерфейс, предназначенный для выполнения функций самообслуживания, включая сброс пароля и управление идентификационными данными. В качестве фундамента для работы FIM Portal используются среда ASP.NET и Microsoft Sharepoint.

За счет того, что портал располагается в среде MS Sharepoint, существует возможность добавления, удаления и изменения элементов на портале. Это дает администраторам возможность более гибкой настройки интерфейса FIM.

Синхронизация учетных данных

FIM может применяться для решения многих задач, но чаще всего используется для управления идентификационными данными каталогов, а именно управление учетными записями пользователей за счет синхронизации атрибутов, таких как имя, фамилия, номер телефона, наименование должности и название отдела. Например, если пользователь получает повышение в должности, изменение должности будет занесено в базы данных отдела кадров и бухгалтерии, а затем, с помощью агентов управления, автоматически реплицировано во все используемые информационные системы организации. Это дает уверенность в том, что название должности пользователя будет выглядеть одинаково во всех системах, которые синхронизируются с помощью FIM. Такой способ применения FIM является наиболее распространенным и называется управлением идентификацией. К числу других распространенных способов использования FIM относятся инициализация учетных записей и управление группами.

FIM позволяет администраторам легко производить инициализацию и деинициализацию учетных записей и идентификационной информации пользователей для множества систем и платформ.

Под инициализацией учетных записей в FIM подразумевается расширенная настройка агентов управления каталогами вместе со специальными агентами инициализации для автоматизации процесса создания и удаления учетных записей в нескольких информационных системах. Например, в случае создания в каталоге Active Directory новой учетной записи пользователя, агент управления Active Directory может пометить ее необходимым образом, чтобы агенты управления других каталогов при запуске автоматически сгенерировали аналогичную учетную запись в других обслуживаемых ими каталогах (системах).

Кроме того, связанные учетные записи пользователей могут в FIM не только автоматически создаваться с помощью процесса инициализации, но и автоматически удаляться или отключаться через процесс деинициализации. Автоматизация процесса удаления связанных учетных записей упрощает администрирование большого количества систем с множеством учетных записей, а также сводит к минимуму риск действующей учетной записи после увольнения сотрудника.

В частности, FIM позволяет администраторам быстро создавать новые учетные записи для сотрудников на основе событий или изменений в авторитетных хранилищах, таких как система отдела кадров, а в случае увольнения сотрудников – немедленно удалять или блокировать использованные ими учетные записи из тех же систем.

Инициализация учетных записей в FIM предоставляет возможность применения усовершенствованных конфигураций агентов управления каталогами вместе со специальными агентами инициализации для автоматизации процесса создания и удаления учетных записей в нескольких каталогах.

Агент управления связывает конкретный подключенный источник данных с метакаталогом (рис. 3) и отвечает за перемещение данных между подключенным источником данных и метакаталогом. При изменении данных в метакаталоге агент может экспортировать данные в подключенный источник данных для поддержания того в синхронизированном с метакаталогом состоянии. Обычно для каждого подключаемого каталога создается, как ми-

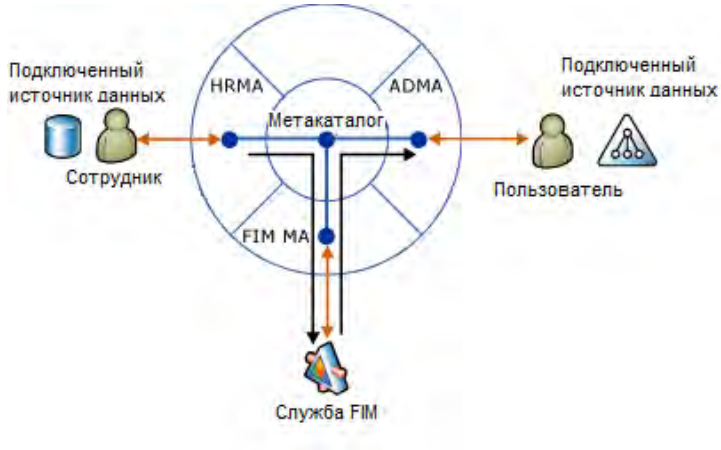

Рис. 3. Синхронизация FIM

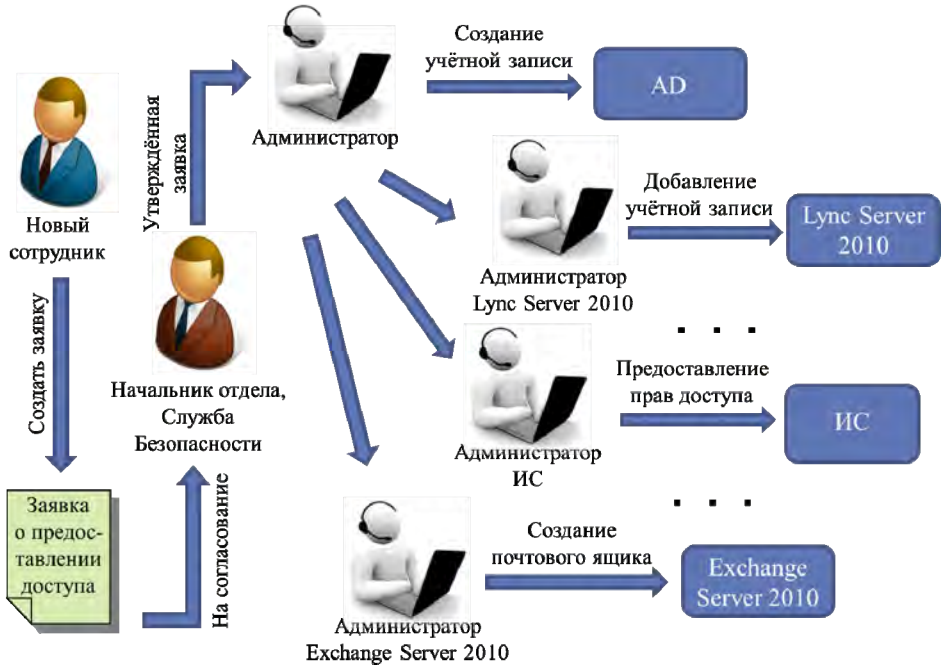

Рис. 4. Предоставление доступа до внедрения FIM

нимум, один агент управления. В общем случае, в FIM допускается создание агентов управления для многих источников каталогов.

Кроме того в FIM предлагается интегрированная поддержка для обеспечения синхронизации с дополнительными каталогами, такими как SAP, Oracle, IBM и Sun.

В агентах управления содержатся правила, которые указывают каким образом должны сопоставляться атрибуты объекта, как объекты подключенных каталогов должны отыскиваться в пространстве имен метастрок и когда объекты подключенных каталогов должны создаваться или удаляться.

Помимо задач, связанных с управлением идентификационными данными учетных записей, FIM может применяться и для решения задач, связанных с управлением группами. При проецировании группы на пространство имен метастрок, атрибут членства в этой группе может реплицироваться в другие подключенные каталоги через их агенты управления. В результате изменение, внесенное в данные о членстве в группах в одном каталоге, автоматически реплицируется в другие каталоги.

Применение Forefront Identity Management 2010 R2 в рамках СВС РФЯЦ-ВНИИЭФ

В результате реализации Программы «Создание Типовой Информационной Системы РФЯЦ-ВНИИЭФ» в РФЯЦ-ВНИИЭФ введена в эксплуатацию новая автоматизированная система «Служебная Вычислительная Сеть (СВС) РФЯЦ-ВНИИЭФ» (АС), объединившая большинство ранее отдельно существующих сегментов локальных сетей предприятия. Данная АС объединяет более 10 000 пользователей и включает в себя различные информационные системы (ИС).

В связи с тем, что каждую ИС обслуживают разные администраторы, поддержка соответствия данных о пользователях в них затрудняется.

До внедрения Forefront Identity Management в СВС РФЯЦ-ВНИИЭФ получение новых и обновление существующих идентификационных данных пользователей занимало достаточно долгое время. Данный механизм работал крайне неэффективно из-за большого количества взаимодействий между администраторами информационных систем (рис. 4).

В связи с этим, появилась необходимость в изменении подхода к обновлению информации о пользователях для поддержания данных в актуальном состоянии во всех системах с минимальными временными и ресурсными затратами.

Результаты, полученные использованием FIM в СВС РФЯЦ-ВНИИЭФ:

1. Автоматизация типовых задач управления учетными записями пользователей, группами и списками рассылки;
2. Сокращение времени предоставления новому сотруднику прав доступа в информационных системах в соответствии с ролевой моделью;
3. Повышение информационной безопасности благодаря мониторингу кадровой базы данных – оперативное получение информации об изменениях ролевых моделей сотрудников, о перемещениях персонала, увольнениях;
4. Уменьшение числа ошибок в учетных данных пользователей.

За главный источник данных была принята база данных кадровой системы РФЯЦ-ВНИИЭФ. С помощью FIM был разработан механизм синхрониза-

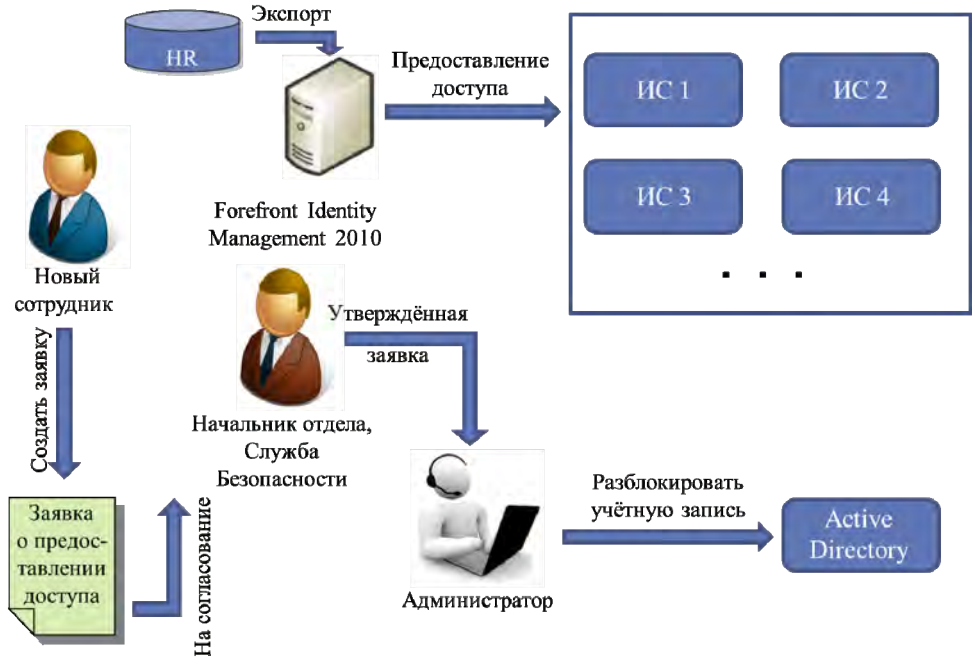

Рис. 5. Предоставление доступа после внедрения FIM

ции кадровой базы с Active Directory домена СВС РФЯЦ-ВНИИЭФ. Синхронизация проводится по расписанию, но также может быть выполнена вручную, в любой момент. Таким образом, любые изменения в учетных данных сотрудников переносятся в каталог Active Directory СВС РФЯЦ-ВНИИЭФ с задержкой не более 7 дней.

Также была решена задача предоставления доступа. В момент синхронизации учетные данные сотрудников, отсутствующие в каталоге Active Directory, автоматически создаются согласно настроенным правилам. При этом, новые учетные записи также создаются в других ИС согласно ролевой модели, например, на почтовом сервере Microsoft Exchange и сервере обмена мгновенными сообщениями Microsoft Lync.

Новые ученые записи пользователей создаются в каталоге Active Directory домена СВС заблокированными, без возможности их использования до момента подписания соответствующего разрешения. Таким образом, после одобрения заявки на доступ, новый сотрудник сразу получает доступ к требуемым ИС (рис. 5). Подобное решение помогает сэкономить время, затрачиваемое администраторами на создание учетных данных в их системах, и самим пользователем, ожидающим предоставления доступа к требуемой ИС. Например, новый сотрудник, только поступивший на работу, уже имеет учетную запись в Active Directory, необходимую для доступа к СЛВС подразделения. Помимо записи в Active Directory, новый работник получает почтовый адрес на сервере Exchange и учетную запись на сервере обмена мгновенными сообщениями MS Lync. Перечень участвующих в этом процессе ИС продолжает расширяться.

При увольнении сотрудника механизм также автоматизирует деятельность администраторов. Когда из базы данных кадров удаляется запись в момент синхронизации происходит блокировка учетной записи в Active Directory. После этого осуществить вход в сеть или получить доступ к почте или сообщениям с помощью данной учетной записи невозможно.

Заключение

В результате внедрения механизма управления учетными записями пользователей у администраторов стало меньше рутинной работы, что сильно сэкономило время. В свою очередь сотрудники не тратят время на ожидание создания или изменения своих учетных данных, что позволят снизить издержки из-за простоя в работе. Любые изменения в учетных данных всех сотрудников предприятия своевременно поступают в основные Информационные системы. За счет частичной автоматизации процесса управления учетными данными, сводится к минимуму кол-во ошибок в данных сотрудников, допущенных из-за невнимательности администратора.

Литература

1. [Electronic resource] Mode of access: https://technet.microsoft.com