

Решения для системного управления



УПРАВЛЕНИЕ ДОСТУПОМ
К ИТ-РЕСУРСАМ

ПРОБЛЕМЫ ИТ

Для выполнения бизнес-задач сотрудники компании часто должны иметь доступ к большому количеству приложений. При реализации традиционного подхода к обеспечению безопасности для сотрудника создается учетная запись в каждом приложении. При этом сотрудник вынужден проходить процедуру аутентификации многократно (многократно вводить имя пользователя и пароль или другие идентификационные данные, использовать биометрические средства и т. п.). Ему приходится помнить множество паролей. Это приводит к записи паролей пользователями, заданию «простых» паролей в системах, что понижает общий уровень безопасности.

При этом существует большое количество несвязанных каталогов пользователей и политик предоставления доступа, которые управляются независимо, что может привести к снижению общего уровня информационной безопасности.

Кроме этого, внедрение любых новых систем предполагает решение задач, связанных с управлением доступом. Отсутствие единой политики и унифицированных средств управления доступом приводит к тому, что компания каждый раз платит за решение одной и той же задачи.

Рост количества информационных систем и использование web-технологий неизбежно приводит к появлению задач, связанных с интеграцией приложений. Решений таких задач зачастую усложняется тем, что каждая система использует свои технологии для защиты данных и управления доступом.

БИЗНЕС-ЗАДАЧИ

Основными бизнес-задачами являются:

- снижение затрат на управление доступом и повышение эффективности работы персонала;
- повышение уровня информационной безопасности;
- упрощение создания и модернизации бизнес-приложений;
- расширение бизнеса за счет предоставления доступа к web-ресурсам компании через Интернет;
- унификация бизнес-правил предоставления доступа к разнородным информационным ресурсам компании;
- снижение рисков несанкционированного доступа.

АКТУАЛЬНОСТЬ РЕШЕНИЯ ЗАДАЧ

Многие крупные компании сталкиваются с такими характерными проблемами отсутствия централизованной системы управления доступом, как длительный срок исполнения заявки на предоставление доступа, необходимость запоминания множества паролей для входа в разные системы, сложность проведения аудита предоставленных прав доступа и другими. При этом компании зачастую применяют системы, позволяющие решить только часть задач, например, системы автоматического согласования заявок и специфические решение по созданию единой процедуры регистрации (Single Sign-ON). Подобные проекты отнимают значительное количество времени и ресурсов, но, как правило, не дают желаемых результатов.

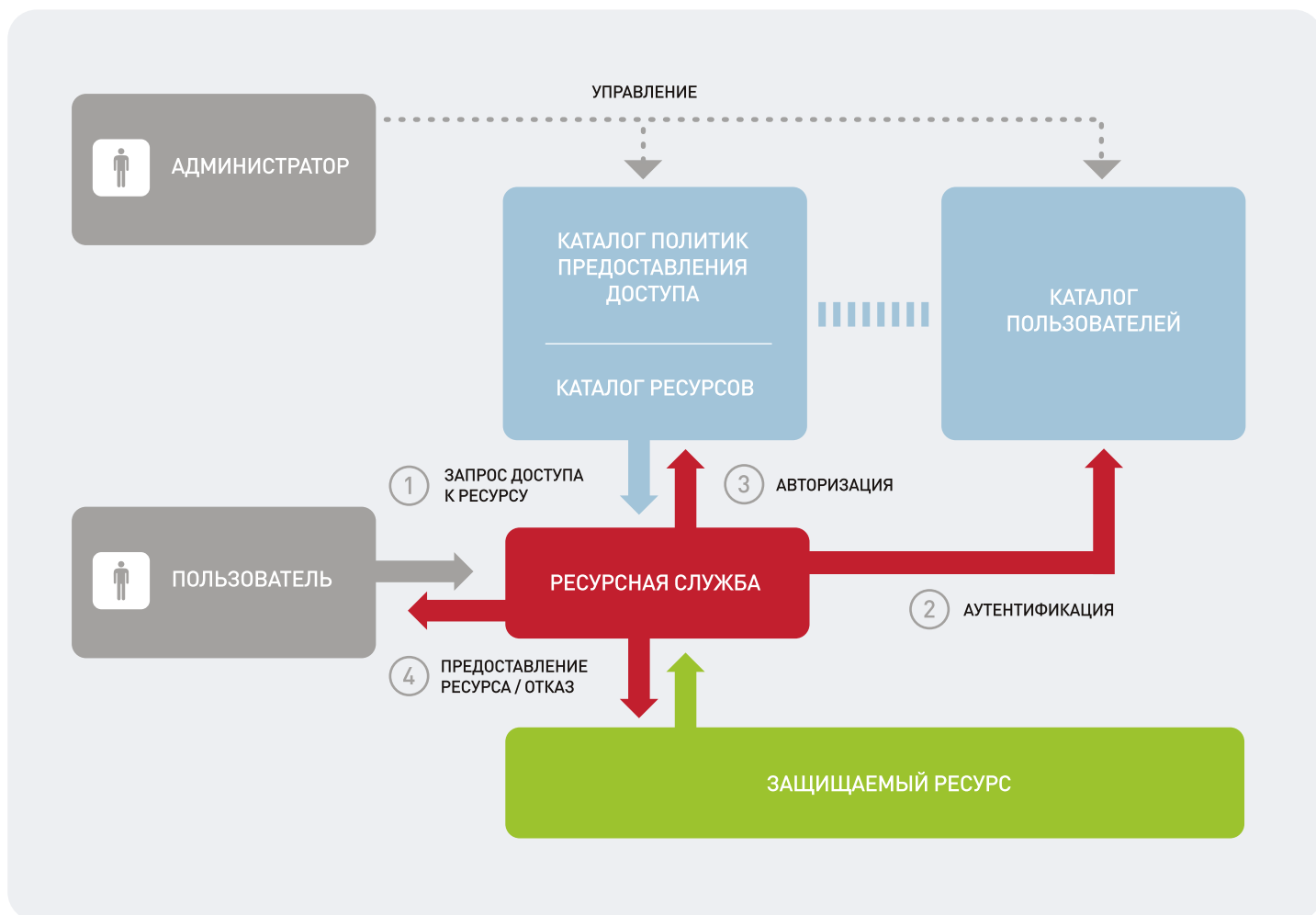
Для предприятий, планирующих создание современной ИТ-инфраструктуры, способной выдержать рост числа пользователей и готовой к появлению новых технологий и стандартов, внедрение централизованной системы управления доступом является стратегической инвестицией. Внедрение подобной системы позволит один раз определить правильный подход к организации доступа к ИТ-ресурсам на предприятии на основе корпоративных политик и политик информационной безопасности, и использовать его в последствии для всех внедряемых решений.

ПРОДУКТЫ, ИСПОЛЬЗУЕМЫЕ ПРИ ПОСТРОЕНИИ РЕШЕНИЯ:

- IBM Tivoli Access Manager,
- IBM Tivoli Identity Manager,
- IBM Tivoli Directory Server,
- IBM Tivoli Directory Integrator.

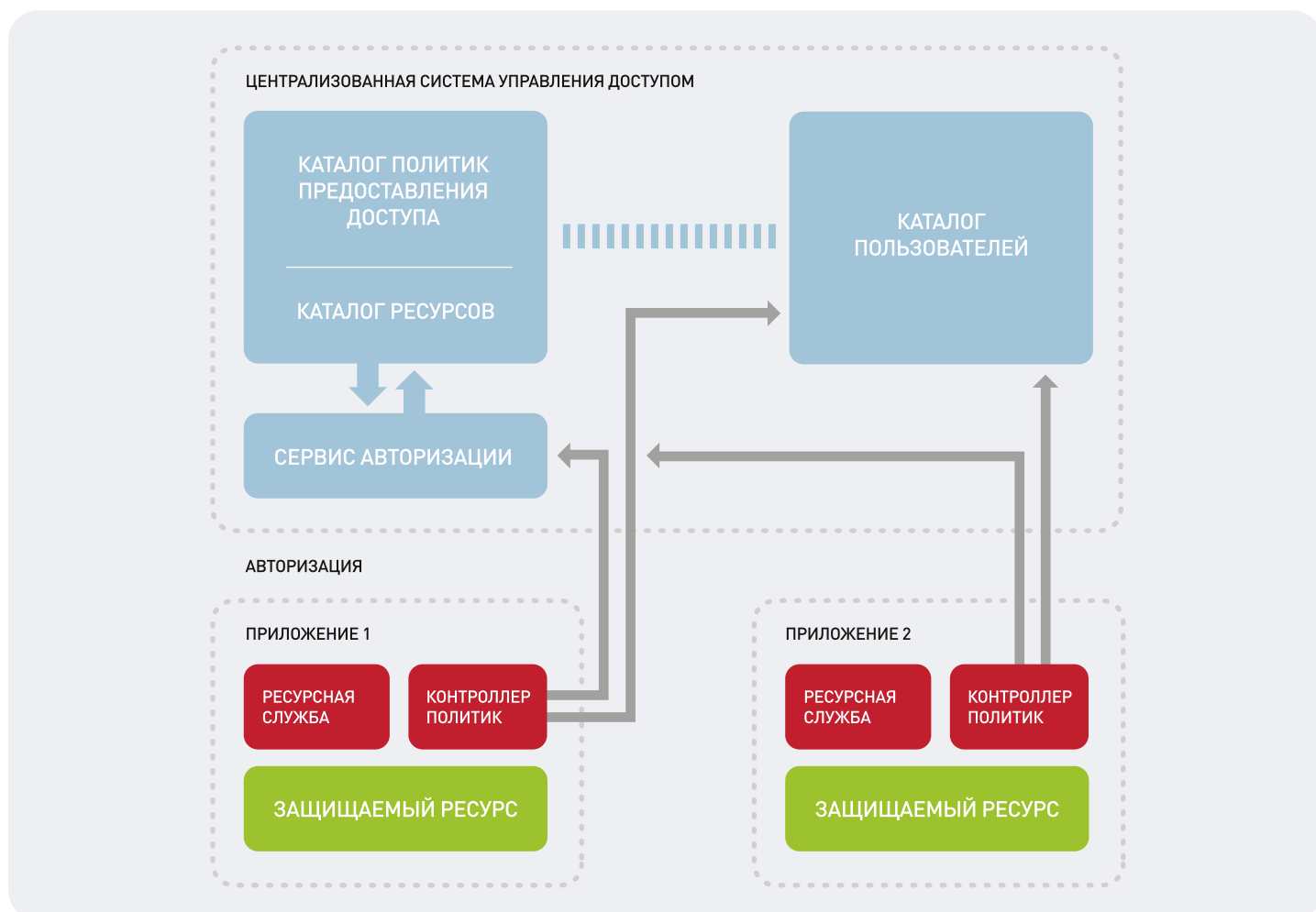
ОПИСАНИЕ РЕШЕНИЯ

Для того, чтобы описать предлагаемое решение, перечислим стандартные механизмы управления доступом, присутствующие в любом корпоративном приложении.



- **Аутентификация** — процедура проверки подлинности предъявленных пользователем идентификационных данных (имени пользователя, пароля, токена, идентификационной карты, ключа).
- **Авторизация** — процедура предоставления пользователю доступа к информационным ресурсам в соответствии с полномочиями данного пользователя на основании политик предоставления доступа.
- **Политики предоставления доступа** — правила, описывающие права пользователя на выполнение операций с информационными ресурсами.
- **Каталог пользователей** — каталог, содержащий учетную информацию о пользователях автоматизированной системы.

При организации централизованной системы управления доступом решение о предоставлении пользователю запрашиваемого ресурса выносится за рамки приложения, содержащего данный ресурс. Создается единая база авторизации и база учетных записей пользователей (УЗП). При этом решение осуществляется на основании этих данных специальным сервисом авторизации.



Логика работы «ресурсной службы» приложения при этом меняется. Возможны два варианта ее функционирования:

- Ресурсная служба приложения «отключается» и не участвует в процедуре предоставления доступа. Все запросы пользователей перехватываются специальным компонентом — контроллером политик, который сам непосредственно защищает ресурс.
- Происходит интеграция ресурсной службы и контроллера политик. Часть функций при этом перекладывается на контроллер политик, а задачи взаимодействия с пользователем и ресурсами по-прежнему решаются через ресурсную службу.

При использовании обоих вариантов контроллер политик играет роль связующего звена с центральной системой управления доступом. При запросе доступа к ресурсу он производит аутентификацию, опираясь на единый каталог учетных записей пользователей, после чего направляет запрос на центральный сервис авторизации. Сервис авторизации принимает решение на основе единой базы политик предоставления доступа и связанный с ней каталог УЗП.

Политики в каталоге, как правило, включают в себя списки контроля доступа. Списки контроля доступа содержат данные о ресурсе, к которому ограничивается доступ, УЗП или группы УЗП и наборы атрибутов, определяющих для каждой УЗП (группы УЗП) права доступа к ресурсу.

При необходимости более детальной настройки правил доступа могут быть использованы также специальные политики. Возможности таких политик и правила их записи зависят от конкретной платформенной реализации. Как правило, они включают в себя некоторый предопределенный набор правил, основанных на расширенных атрибутах УЗП, а также встроенный язык для описания новых правил.

После того, как сервис авторизации определит права доступа пользователя к запрашиваемому ресурсу, информация об этом передается обратно контроллеру политик, который на основе полученных данных предоставляет доступ пользователя к ресурсу.

Наличие централизованной системы управления доступом позволяет удешевить и упростить ввод в эксплуатацию новых программных компонентов. Разрабатываемые компоненты должны лишь удовлетворять требованиям интеграции, которая производится на основе открытых стандартных протоколов. Таким образом, отсутствует необходимость разработки собственных модулей обеспечения безопасности для новых компонентов.

К самой системе при этом предъявляются требования открытости и масштабируемости архитектуры, поскольку она является одной из наиболее критичных систем предприятия. Поэтому предполагается строить ее на базе открытых стандартов и протоколов. Организация модели доступа на базе предлагаемой архитектуры позволяет поддерживать использование современных методов аутентификации и авторизации (X.509 Certificates, NTLM, Kerberos, TAI, Basic Authentication и др.).

В настоящее время практически все автоматизированные системы строятся на основе web-сервисов. Описываемое решение имеет встроенные механизмы интеграции с приложениями, построенными на базе web-технологий.

РЕАЛИЗАЦИЯ РЕШЕНИЯ НА БАЗЕ ЛИНЕЙКИ ПРОДУКТОВ IBM TIVOLI

Для реализации механизмов управления доступом используется IBM Tivoli Access Manager (ITAM). Данный продукт позволяет создавать единый каталог пользователей и базу политик предоставления доступа.

Политики доступа в Tivoli Access Manager реализуются с помощью следующих механизмов:

- Списки контроля доступа, которые реализуют разграничение доступа к ресурсу на уровне прав пользователей и групп пользователей.
- Политики защищаемого объекта. Разграничение прав доступа на уровне свойств объекта и параметров доступа (таких, как время доступа, IP-адрес компьютера, с которого осуществляется доступ и т. п.).
- Правила авторизации, позволяющие настроить специальные условия доступа, основанные на дополнительных атрибутах. Правила авторизации реализуются в системе при помощи XSLT-преобразований (при этом атрибуты поступают на вход правила в виде специального файла в формате XML).

В состав Tivoli Access Manager входит набор готовых контроллеров политик для типовых защищаемых ресурсов (серверов web-приложений, UNIX-операционных систем, приложений .NET и др.). Данные компоненты представляют собой некоторую надстройку (plug-in) над защищаемой системой.

Защита web-приложений возможна также с использованием специального компонента WebSeal, который представляет собой реверсивный прокси-сервер и реализует защиту доступа к данным на уровне фильтрации запросов HTTP.

Запрос авторизации также может передаваться при помощи API - функций, реализованных в Tivoli Access Manager в виде Java - классов и библиотек языка C. Такой механизм позволяет интегрировать в единую систему предоставления доступа приложения сторонних производителей и упрощает разработку новых приложений.

В случае наличия автоматизированных систем, модификация которых не представляется возможной, централизация может быть осуществлена при помощи создания мета - каталога пользователей (каталога, который содержит список учетных карточек пользователя, объединяющих информацию обо всех учетных записях пользователя в различных автоматизированных системах).

Данный механизм реализуется при помощи продукта IBM Tivoli Identity Manager. IBM Tivoli Identity Manager позволяет централизованно осуществлять наполнение каталогов автоматизированных систем с помощью специальных программных адаптеров. Логика работы ресурсных служб самих систем при этом не меняется.

Совместное использование продуктов Tivoli Access Manager и Tivoli Identity Manager позволяет построить единую систему аутентификации и авторизации пользователей (на базе продукта Tivoli Access Manager) и организовать централизованное управление всеми автоматизированными системами (на базе продукта Tivoli Identity Manager). При этом Tivoli Access Manager является управляемой системой по отношению к Tivoli Identity Manager наравне с остальными автоматизированными системами предприятия.

ПЕРСПЕКТИВЫ РАЗВИТИЯ РЕШЕНИЯ

Использование предлагаемого решения позволяет в дальнейшем существенно наращивать его функциональность за счет выполнения таких задач как:

- интеграция с системами учета кадров для автоматического формирования каталога пользователей;
- автоматическое предоставление доступа пользователям на основе функциональной позиции пользователя в организации (ролевая модель) или автоматическое исполнение заявки на предоставление доступа пользователю (прецедентная модель);
- использование принципов федеративности (federated identity management) для организации прозрачного для пользователя доступа к автоматизированным системам предприятий, входящих в единый холдинг.



ПРИМЕР ВНЕДРЕНИЯ

- ОАО «ВымпелКом»

COMPUTEL SYSTEM MANAGEMENT

- КОНСАЛТИНГ
- ПРОЕКТИРОВАНИЕ
- ВНЕДРЕНИЕ
- ТЕХНИЧЕСКАЯ ПОДДЕРЖКА
- УЧЕБНЫЙ ЦЕНТР IBM TIVOLI

115184, Москва,
ул. Б. Татарская 35, стр. 5

тел.: + 7 (495) 234-1931
info-tivoli@computel.ru

www.computel.ru
www.tivoli.computel.ru