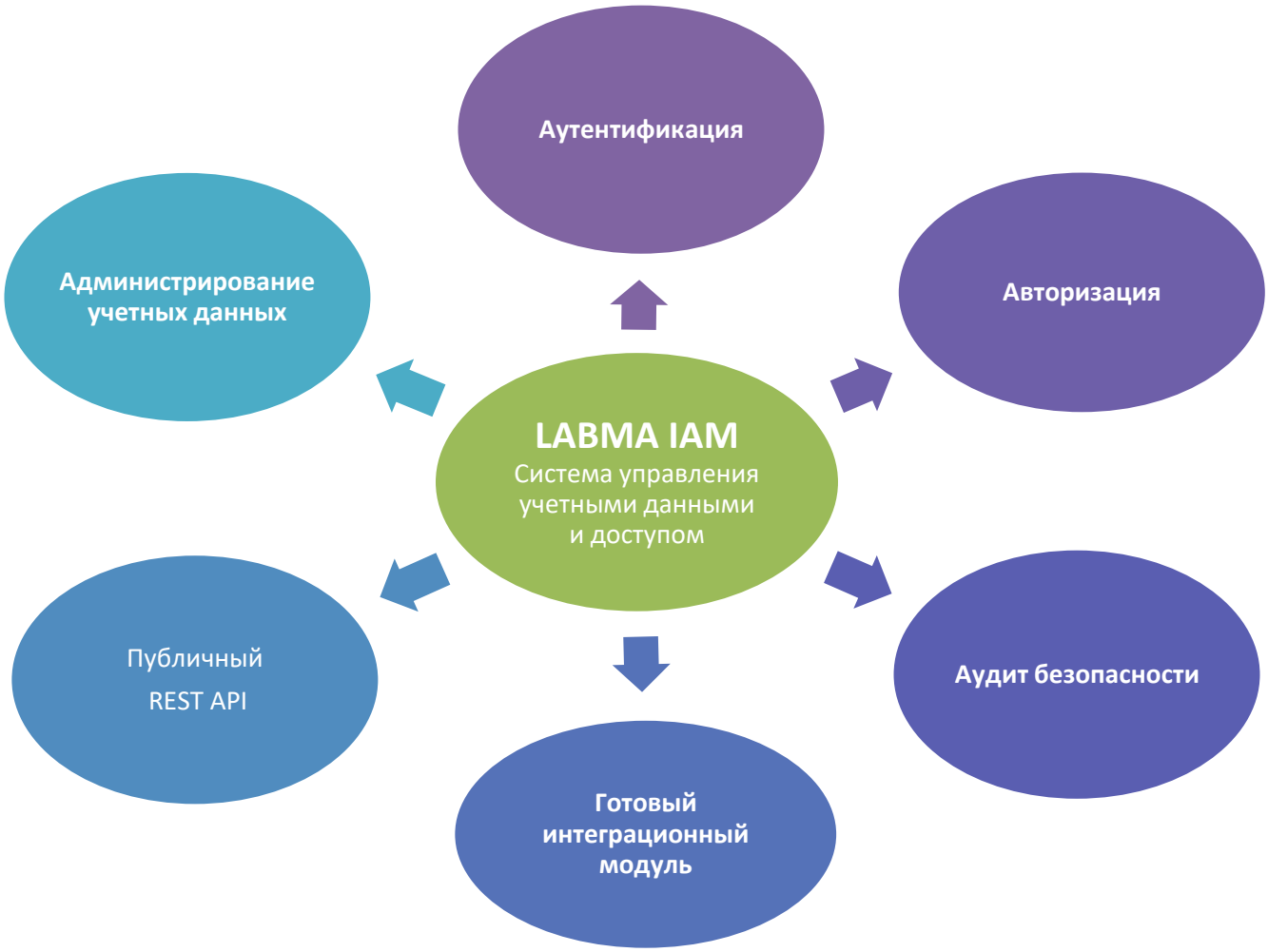
LABMA IAM

Система управления учетными данными и доступом

LABMA IAM – программная система класса Identity and Access Management. Она предназначена для централизованного и гибкого управления правами доступа к различным корпоративным приложениям и сервисам. LABMA IAM обеспечивает аутентификацию в соответствии со стандартом OpenID Connect и авторизацию по протоколам OAuth 2. Поддерживаются различные модели управления доступом: на основе ролей (RBAC) и на основе списков управления доступом (ACL).

Общая функциональная структура системы LABMA IAM показана на диаграмме. Более подробно функции и компоненты системы описаны ниже.



Администрирование учетных данных

В LABMA IAM с помощью специальных визуальных инструментов выполняется администрирование основных сущностей системы: приложения, роли, разрешения, группы, пользователи, подразделения.

В системе регистрируются приложения, для которых необходимо обеспечить разграничение доступа, для них описываются или импортируются списки поддерживаемых разрешений.

Поддерживаются различные модели управления доступом – Role Based Access Control (RBAC) и Access Control List (ACL).

RBAC обеспечивает управление доступом на основе ролей. Роли могут быть как простыми, так и составными, формируемые из набора поддерживаемых разрешений. Для удобства роли могут объединяться в группы. Назначение пользователю прав доступа возможно через группу, роль или конкретное разрешение.

ACL – список правил, представляющих собой специальные разрешения, определяющих правила доступа субъекта (приложения или пользователя) к конечным экземплярам объектов.

Для пользователей поддержаны ведение ключевых атрибутов (логин, ФИО, почта и т.д.), а также привязка к организационно штатной структуре организации путем выбора соответствующего подразделения.

Для подразделений также поддержано ведение ключевых атрибутов (наименование, индекс, дата формирования и т.д.). Структура подразделений описывается в виде дерева. Поддерживаются функции упразднения подразделения (с возможностью указать подразделение-преемник), удаления подразделения (с сохранением истории или без) и др.

Для пользователей и подразделений поддерживается гибкое ведение расширенных атрибутов, специфичных для конкретной организации.

Аутентификация

LABMA IAM является единой точкой аутентификации для всех внешних приложений и обеспечивает технологию единого входа (SSO - Single Sign-On) и единого выхода (SLO - Single Logout).

Подключение приложений к LABMA IAM происходит с использованием стандарта безопасной аутентификации OpenID Connect.

По умолчанию, поддерживается аутентификация с использованием ввода логина и пароля для зарегистрированных пользователей. При встраивании в корпоративный IT-ландшафт организации в LABMA IAM могут быть настроены и другие методы аутентификации:

- использование HTTP-заголовка внешнего доверенного веб-сервера;
- использование протокола Kerberos;
- использование протокола LDAP.

Все успешно аутентифицированные пользователи получают токены доступа в соответствии со стандартом JSON Web Token.

Авторизация

В состав LABMA IAM входит сервер авторизации, который поддерживает современный протокол OAuth 2. Сервер авторизации обеспечивает:

- выдачу подписанных токенов доступа аутентифицированным пользователям или зарегистрированным приложениям в соответствии со стандартом JSON Web Token (JWT);
- выдача публичных ключей для валидации токенов доступа (проверка подписей);
- выдачу информации о пользователе и его правах для доступа к защищенным ресурсам внешних приложений на базе передаваемого токена доступа.

Аудит безопасности

LABMA IAM фиксирует в журнале аудита следующие события безопасности:

- создание/изменение/удаление основных сущностей системы;
- события входа/выхода из системы, в том числе попытки несанкционированного доступа;
- операции с самим журналом аудита (создание архивного журнала, удаление журнала).

Предоставляются возможности поиска и просмотр событий в разрезе необходимых операций, пользователей, подразделений, времени, даты и т.д. Для найденных записей доступна выгрузка для последующей печати.

Система также поддерживает автоматический или ручной перенос событий безопасности в архив.

Публичный REST API

В LABMA IAM имеется публичный REST API, разработанный в соответствии со стандартом OpenAPI 3.0.

REST API содержит методы, используемые в процессе аутентификации и авторизации, а также методы для ведения всех основных сущностей системы, которые могут быть использованы для задач их импорта/синхронизации из существующих системам организации.

В составе LABMA IAM доступна специальная страница для разработчиков внешних приложений (в формате Swagger), позволяющая получить актуальное описание методов, а также произвести их тестовые вызовы.

Для реализации на стороне приложений сервисов по взаимодействию с LABMA IAM предоставляется описание API в формате OpenAPI 3.0.

Готовый интеграционный модуль

Для приложений, построенных с использованием Spring Framework, предоставляется готовый интеграционный модуль на базе Spring Security. Интеграционный модуль встраивается в приложение, предоставляя ему сервисы аутентификации и авторизации LABMA IAM.