

Идентификация и аутентификация пользователей

Что не так с доступом к вашим приложениям?

Михаил Ванин

Генеральный директор «РЕАК СОФТ»

Mvanin@reaxoft.ru

ВЫСШАЯ ШКОЛА ЭКОНОМИКИ

ИТ-ландшафт в Высшей школе экономики

Приложения

- электронная почта/календарь
- ИС «Личный кабинет сотрудника»
- ИС «Информационная образовательная среда НИУ ВШЭ»
- более 30 облачных ресурсов: JSTOR, Web of Science, eLibrary.ru и др.
- системы бэк-офиса: учет контингента, бухгалтерия и др.

Категории пользователей

- администрация (~250)
- преподаватели (~2 500)
- студенты (~25 000)

Особенности доступа

- преподаватели и студенты используют собственные устройства
- различные типы устройств: ПК, планшеты, смартфоны
- доступ из внутренней сети и из Интернет

Ожидания и реальность



Ожидания

- удобство пользователей
- безопасность
- контроль



Реальность

- отторжение со стороны пользователей
- низкая защищенность
- слабый контроль

Кто виноват?



Пользователи

Испытывают сложности с доступом, парольный хаос



Заказчик

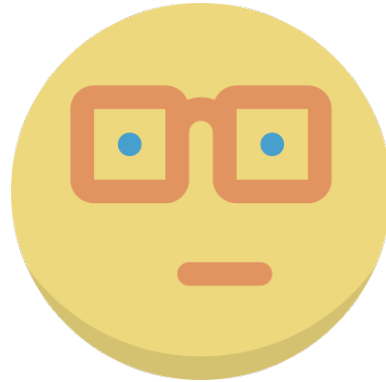
Имеет много приложений, в каждом из которых контроль доступа реализован по своему



Консервативный разработчик

Считает идентификацию и аутентификацию пользователей внутренней функцией своего приложения

Что делать?



Приложения не должны самостоятельно осуществлять идентификацию и аутентификацию своих пользователей
Это задача специализированного сервиса организации

Единый сервис доступа – это в тренде



Единый сервис доступа – это в тренде

The screenshot shows the RIA Novosti website with a login modal titled "АВТОРИЗАЦИЯ". The modal contains fields for "E-mail" and "Пароль", a "ВОЙТИ" button, and a "Помнить меня" checkbox. Below these are social media login options for Facebook, Twitter, and Google+. The background shows the website's navigation menu and news articles.

The screenshot shows the Svyaznoy website with a login modal titled "Авторизация". The modal contains fields for "Эл. почта или логин" and "Пароль", a "ВОЙТИ" button, and a "Запомнить меня!" checkbox. There are also social media icons and a "Забыли пароль?" link. The background shows the website's navigation menu and product listings.

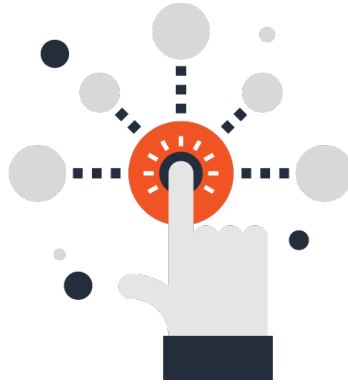
The screenshot shows the Beeline website with a login page titled "Вход в личный кабинет «Мой Билайн» для физических или юридических лиц". The page features a "Вход через соцсети" section with buttons for Mail.ru, Facebook, LinkedIn, and Google+. There is also a "Вход через" section with social media icons. A yellow banner at the bottom reads "Новые возможности" and "Теперь вы можете с легкостью следить за расходами, подключать услуги, узнавать все о своем тарифном плане, а если у вас и номер не один - управлять всеми!".

Требования к единому сервису доступа



Подключение к существующей базе пользователей

- к контроллеру домена Active Directory / Samba
- к любому LDAP-каталогу
- к реляционной БД



Простота подключения приложений

- соответствие стандартам:
- SAML 2.0
 - OAuth 2.0
 - OpenID Connect 1.0



Гибкость настройки методов аутентификации

- поддержка различных методов усиленной и строгой аутентификации
- поддержка устройств различных производителей

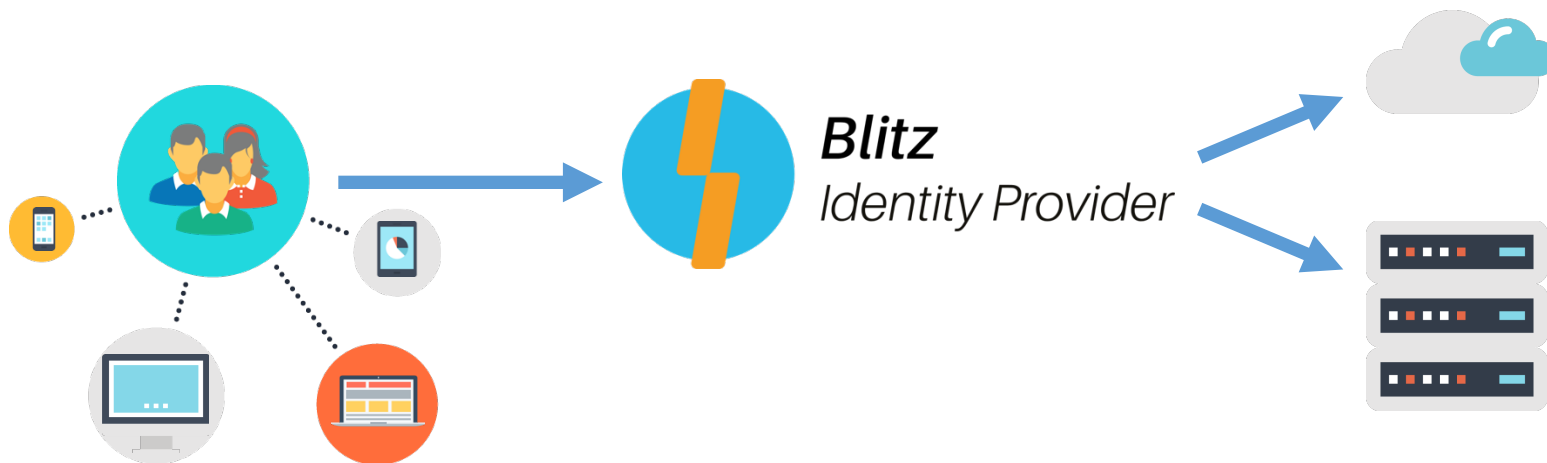
Единый сервис доступа для вашей организации



Blitz

Identity Provider

Единый сервис доступа для вашей организации



Пользователи с использованием любых устройств
проходят идентификацию и аутентификацию

Получают доступ к приложениям
как внутри, так и вне организации

Заключение

1. Не позволяйте разработчикам приложений ограничиваться встроенными функциями идентификации / аутентификации пользователей
2. Создайте единый сервис доступа пользователей к приложениям вашей организации
3. Посмотрите демонстрацию нашего программного продукта – Blitz Identity Provider