# ВЕБ-ПРИЛОЖЕНИЕ «SINGLE SIGN ON» ДЛЯ ДОСТУПА К УЧЕТНЫМ ДАННЫМ ПОЛЬЗОВАТЕЛЯ ACTIVE DIRECTORY

*Дергай И.С.*

*Белорусский государственный университет информатики и радиоэлектроники*
*г. Минск, Республика Беларусь*

*Виничук О.Н., Славинская О.В. – канд. пед. наук, доцент*

Технология единого входа (SSO) – это средство аутентификации, позволяющее пользователям осуществлять доступ к нескольким приложениям с помощью одного набора учетных данных. Обычно организации используют технологию единого входа для упрощения доступа к различным приложениям на стороне потребителя, веб- и облачным приложениям с целью повышения комфортности работы пользователей. Она также может предоставить ИТ-отделу расширенный контроль пользовательского доступа, сократить число обращений в службу поддержки в связи с паролями, а также улучшить безопасность и соответствие стандартам. Наша статья описывает разработанное нами веб-приложение «Single Sign On» для доступа к учетным данным пользователя Active Directory.

Сегодня приложения развертываются в центрах обработки данных и облаках, а также доставляются в виде SaaS-приложений. Каждое бизнес-приложение предусматривает прохождение пользователем процедуры аутентификации перед получением доступа к тому или иному ресурсу. Ранее, до появления технологии единого входа, пользователям приходилось выполнять вход при помощи набора учетных данных каждый раз, когда требовалось переключаться между приложениями. В большинстве случаев для каждого приложения был предусмотрен отдельный набор учетных данных, результатом чего являлось снижение комфортности работы пользователей, невозможность получения доступа к нужным ресурсам из-за забытого логина или пароля, неоднородность политик контроля доступа и увеличение расходов на поддержку этих приложений.

Технология единого входа является компонентом системы управления федеративными удостоверениями (FIM) межорганизационной структуры, позволяющей подписчикам использовать одни и те же идентификационные данные для доступа к сети каждой организации.

Идентификация пользователя происходит в нескольких доменах безопасности, в каждом из которых имеется собственная система управления средствами идентификации. При федерации доменов пользователь может пройти аутентификацию в одном из них и осуществлять доступ к ресурсам в другом без необходимости повторно выполнять вход.

Схема, позволяющая сторонним организациям, например, LinkedIn или Facebook, использовать чьи-либо данные учетной записи для выполнения входа без раскрытия пароля, называется OpenID Connect. Она служит посредником, предоставляя сервису токен, позволяющий делиться данными только конкретной учетной записи. Когда пользователь осуществляет доступ к приложению, сервис отправляет запрос аутентификации поставщику идентификации, который проверяет запрос и предоставляет доступ. SSO-сервисы на базе SAML обмениваются данными аутентификации и авторизации пользователей в безопасных доменах и управляют связью между пользователем, поставщиком идентификации с каталогом пользователей и поставщиком услуг.

Active Directory – служба каталогов от корпорации Microsoft. Системные администраторы используют технологию Active Directory в Windows Server для хранения и организации объектов в сети в иерархическую защищенную логическую структуру, например, пользователей, компьютеров или других физических ресурсов. Active Directory нужен для хранения информации о ресурсах компании (компьютерах, пользователях, принтерах и т.п.) и предоставляет следующие возможности:

- сервис аутентификации (проверки логина и пароля);
- массовое распространение настроек всем пользователям и компьютерам сети;
- база данных для хранения настроек совместимых приложений.

Основным назначением разработанного веб-приложения является реализация единой точки входа пользователей через учетные данные Active Directory.

Разработанное веб-приложение позволяет решить следующие задачи:

- повысить безопасность и облегчить работу пользователя благодаря уменьшению количества хранимых паролей;
- уменьшить затраты времени на аутентификацию в каждом сервисе;
- упростить администрирование учетных записей;
- облегчить внедрение технологии повышения безопасности благодаря использованию единого провайдера аутентификации для различных операционных систем и устройств.

Входными данными для разрабатываемого программного средства являются учетные данные пользователей Active Directory.

Выходными данными разрабатываемого программного средства является система авторизации пользователей Active Directory для контроля доступа к ресурсам приложения посредством использования технологии Single Sign On на основе Web Services Federation, OpenID Connect, Saml2P протоколов. На рис. 1 отображена диаграмма, отображающая данную систему.

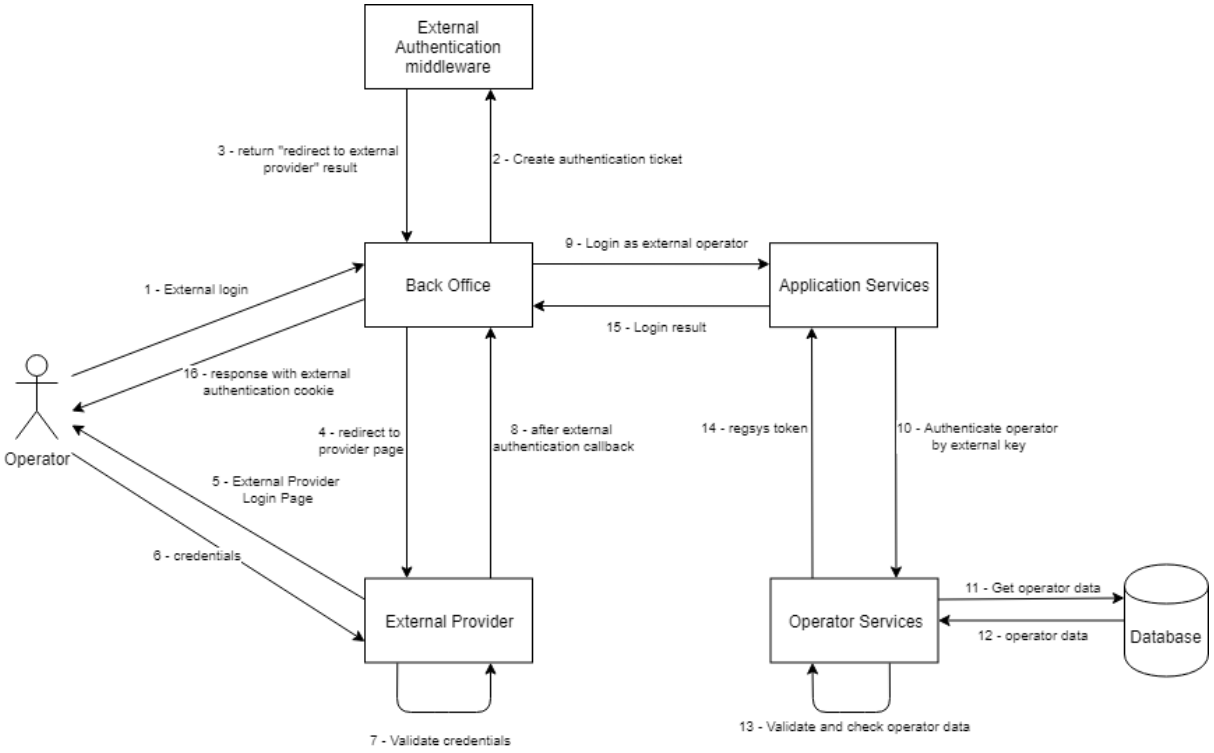


Рис. 1 Диаграмма системы авторизации пользователей с использованием технологии SSO

При создании программного средства были использованы следующие средства разработки:

- Microsoft Visual Studio 2019;
- язык программирования C#;
- JavaScript-библиотека jQuery;
- язык управления реляционными базами данных SQL.

Основным преимуществом данного веб-приложения является возможность настройки технологии Single Sign On на различных протоколах (Web Services Federation, OpenID Connect, Saml2P).

Разработанное веб-приложение дает преимущества как пользователям, так и ИТ-отделу.

С точки зрения пользователей технология SSO облегчает управление паролями, упрощая и ускоряя доступ к приложениям.

ИТ-отделу данное программное средство помогает уменьшить число обращений в службу поддержки в связи с паролями. А автоматическое управление учетными данными сокращает объем ручного управления доступом сотрудников к приложениям и сервисам.

Кроме того, с точки зрения безопасности разработанное веб-приложение может снизить угрозу кибератак, например, фишинга, за счет уменьшения количества подверженных риску учетных данных.

***Список использованных источников:***

*1. Что такое технология единого входа (SSO)? // Citrix [Электронный ресурс]. – Режим доступа : https://www.citrix.com/ru-ru/glossary/what-is-single-sign-on-sso.html.*

*2. Использование технологии единого входа (single sign-on) // Academy.terrasoft [Электронный ресурс]. – Режим доступа : https://academy.terrasoft.ru/documents/administration/7-15/ispolzovanie-tehnologii-edinogo-vhoda-single-sign.*

*3. Структура хранилища Active Directory // 1cloud [Электронный ресурс]. – Режим доступа : https://1cloud.ru/help/windows/struktura-hranilischa-active-directory.*

*4. Что такое Active Directory // Dmosk [Электронный ресурс]. – Режим доступа : https://www.dmosk.ru/terminus.php?object=ad.*